A NEW SYSTEMS APPROACH TO SAFETY MANAGEMENT WITH APPLICATIONS TO ARCTIC SHIP NAVIGATION

by

© Doug Smith

A Thesis submitted to the

School of Graduate Studies

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Faculty of Engineering and Applied Science

Memorial University of Newfoundland

May 2019

St. John's Newfoundland

ABSTRACT

This research is intended to improve the techniques available to safety assessors and provide tools for decision making in safety management. This is done by fostering a new paradigm for safety management, which forms the basis for the performance measurement and process mapping/monitoring (PMPM) method. The research examines safety management philosophies and compares methods, including fault trees, Bayesian Networks, and the functional resonance analysis method (FRAM). This examination is intended to provide a broad understanding of the fundamental safety and risk concepts. The understanding provides the background knowledge to undertake an adaptive safety approach for an Arctic shipping application. The FRAM was adopted for Arctic ship navigation: where three captains were interviewed to form the basis for a functional map of the way ship navigation work can be performed. Also, variations in the ways ship navigation work is performed was recorded from the captains to help understand some of the ways captains may adjust their work to the dynamic conditions they face. Two additions to the FRAM are presented in this work: 1) functional signatures and 2) system performance measurements. Functional signatures provide a method for assessors to animate the FRAM and visualize the functional dynamics over time. System performance measurement provides a way to bring an element of quantification to the FRAM. Quantification can then be used to help compare different scenarios and support decisions. These additions to the FRAM have been demonstrated using data from an ice management ship simulator experiment. The demonstration can be used as a basis to continue future

analysis of using this method in the maritime domain or transfer this approach to other domains.

ACKNOWLEDGEMENTS

I would like to acknowledge the guidance provided by my supervisors, Dr. Brian Veitch, Dr. Faisal Khan, and Dr. Rocky Taylor. Their wealth of knowledge in their respective fields have been instrumental in guiding this research project. Their diverse backgrounds have brought about questions that have forced me to look at this research problem from many different perspectives, in turn strengthening the final product. It has been a pleasure to work with each of them on this project.

The financial support of the Lloyd's Register Foundation is acknowledged with gratitude. Lloyd's Register Foundation helps to protect life and property by supporting engineering-related education, public engagement and the application of research.

Thanks to all the participants who volunteered for the experimental study. This work would not be possible without their interest and time. Also, thanks to the NSERC-Husky Energy IRC in Safety at Sea for financially supporting the experiment and to Erik Veitch for sharing experimental results and collaborating on a manuscript in this thesis.

I would like to thank my colleagues in the LRF Scenario-based risk management for Arctic shipping and operations group and the Safety at Sea group for their support and discussions.

Last but not least I am thankful to the love and support of my family and friends during the time I have been working on this research project.

Table of Contents

List of Tables

List of Figures

1. INTRODUCTION

1.1. Problem statement

Historically, shipping in the Arctic has been limited compared to shipping in more temperate regions. The Arctic contains large seasonal variabilities in environmental conditions, such as ice conditions, air temperature, and daylight. The conditions in the winter season are challenging for vessels to transit and has largely been reserved for specialized vessels. However, the summer season offers a window of opportunity for a larger number of less capable ships to transit the water ways safely. In recent years, a trend of lessening sea ice in the Arctic has been observed (Arctic Council, 2009; Moore et al., 2018; Petty et al., 2018; Petty, 2018). This trend has made the window of opportunity larger for less capable ships to transit the Arctic, which has led shipping companies to consider using the Arctic as a viable alternative to their traditional routes. Coincidentally, shipping traffic in the Arctic has increased in recent years and that trend is expected to continue (Marchenko, 2015). Considering the limited experience of ship operators transiting the Arctic, the projection of increased shipping in the Arctic brings about concerns about safety and the impact it could have on the environment.

A project was awarded by the Lloyd’s Register Foundation (LRF) to a consortium of universities (Memorial University of Newfoundland, Aalto University, University of Helsinki, Norwegian University of Science and Technology, and Hamburg University of

Technology) to investigate areas of uncertainty regarding Arctic shipping risks. The project has a large scope that covers a number of risk related topics with respect to Arctic shipping. The topics in the project address both the probability and consequence elements of the risk framework, including accident prevention, hull structure, ship systems, ice load modelling, harsh climate and weather operations, accident consequence characterization, oil spill modelling, ecosystem response to oil spills, of the risk framework. This thesis dissertation focusses on the accident prevention element.

In the risk framework, improvements in accident prevention can translate to lower likelihood of accidents, thus reducing the risk to Arctic going ships and the environment. Accident prevention in Arctic shipping has many uncertainties that stem from the limited experience and harsh, dynamic operational conditions. There are many areas that improvements in understanding can be made to the prevention of shipping accidents, including, ship technologies, human factors, organizational factors, and environmental factors. It should also be noted that addressing the uncertainties of each of these areas individually may result in an over-simplified understanding of accident processes. These inter-relations are a source of uncertainty that should be addressed to obtain a more thorough understanding of accident processes. The main goal of this thesis is to address some of these uncertainties regarding accident prevention in Arctic shipping to help better inform the larger risk model for Arctic shipping.

1.2. Overview of safety management

Before jumping straight to examining shipping accident processes, it is important to consider some approaches to and philosophies of safety management because they will determine what one might look for as one assesses various processes, and will ultimately affect how one may manage safety. Consider the evolution of industrial safety as put forth by Hale & Hovden (1998): the three ages of industrial safety. Hale & Hoven state that since the industrial revolution (and up until roughly 1998), safety has evolved and can be characterized by 3 ages: the age of technical factors, the age of human factors, and the age of safety management. The age of technical factors began in the late 1800s, the age of human factors began in the late 1960s, and the age of safety management began in the early 1990s, where each age has not replaced the preceding age but rather it has built on to it, thus increasing the scope and complexity of assessments. In recent years, the scope and complexity of safety assessments has continued to increase, which Glendon et al. (2006) has characterized as the integrative age. The integrative age has continued to add factors that build on past assessments to produce more complex, albeit more comprehensive models.

The evolving nature of safety management has resulted in many changes, but one common theme is that the focus of assessments has been on accidents. More and more factors have been deemed important to safety assessments by considering accidents as the focal point of assessments. Hollnagel (2014) argued that safety is the absence of accidents and to make accidents the primary focus for study is inconsistent with the way we investigate other topics in science. For instance, chemistry makes chemicals the focal point of study, and biology makes living organisms the primary focus, not their absence. To study safety in a manner akin to other areas of science research, it would be appropriate to also consider safe operations as a focal point.

Examining safety through safe operations has forced assessors to think more broadly about the mechanisms that may lead to success or failure. Borys et al (2009) have said that this new perspective has brought about a new age, the adaptive age. In this age adaptation is no longer only seen as a failure causing mechanism, it is also essential to success. This new age of safety is just beginning and offers many opportunities to contribute new knowledge. New contributions made in this age will give safety assessors a chance to view operations through this lens and determine the practical utility of this approach. As the understanding of adaptation in operations increases, it may offer more effective holistic management approaches. A timeline of the ages of safety can be seen in Figure 1.1, depicting how each age has built on the previous age.

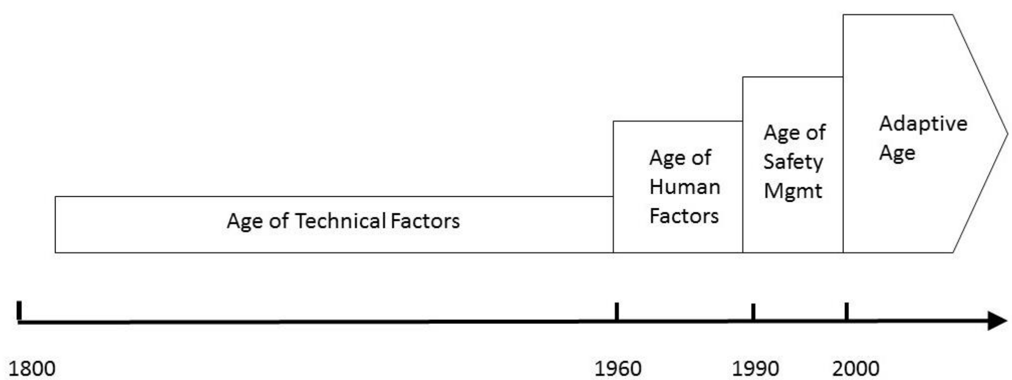


Figure 1.1: Timeline of the ages of safety

Some profound limitations in the management of safety have been discussed by Aven et al. (2015). Stating that current risk frameworks have difficulty dealing with deep uncertainty, surprises, and the unforeseen. Aven et al. (2015) also posit that, in dynamic operations, it may not be appropriate to prescribe a single solution to manage risks. Rather, it may be more appropriate to prescribe a dynamic set of solutions to adapt to the changing conditions. The broader perspective of examining all outcomes of an operation when considering safety or risk, which is characteristic of the adaptive age, has potential to address these issues by understanding how processes are managed over a wide range of outcomes.

Also in conventional risk assessment methods, operations are modelled as a collection of components that can contribute to operational success or failure, both individually and collectively. Again these traditional approaches perform well in well-defined and well-understood situations. Operations that are made up of mainly technical components are the most well-suited to these conventional methods as relationships between components are more linear and it is easier to estimate the collective effect of components. However, systems with more human interactions have been harder to predict using conventional methods (Perrow, 1984). This may be because relationships between technologies and humans are more complicated. Vicente (2004) has attributed the lack of understanding of relationships between technologies and humans to the reductionist approach adopted by the scientific community (and implicitly by society). In the reductionist approach, the scope of problems can be reduced by excluding anything outside of the investigator's purview. This technique is effective for studying narrow scope problems and has allowed many great discoveries in science. Since this approach is the most commonly adopted in the scientific community, most of our collective knowledge is divided in specific domains, each encompassing a great depth of knowledge but, with poorly understood relationships between domains. The humanities and technological sciences are typically investigated separately, and thus knowledge about relationships between these domains is low.

An underlying philosophy of the adaptive age is that adaptation is present in successes and failures of an operation, which has implications about how operations should be managed. Operational adaptation should not necessarily be eliminated or minimized to improve safety, rather adaptation should be understood in specific sets of operational conditions, and minimized or constrained when appropriate. The limited understanding that exists around the new adaptive approach has led others to explore concepts of resilience in safety and risk contexts. In this context, adaptation within industrial applications can be seen as a source of resilience, allowing the operation to persist when subjected to adverse conditions. Qualitatively, adaptation has been observed as a source of resilience in industrial applications but it has been difficult to measure.

Ayyub (2014) proposes using system performance measurement as a signal that can lend quantification to resilience. By tracking system performance over time, assessors can gain a sense of the level of performance that is being achieved. This may allow the assessor to answer questions such as: is the system achieving high performance?, Is the system experiencing losses?, And does the system recover quickly after losses? Answering these questions may provide information that can help understand the level of resilience that is present in a given system. This is important information for managing an operation. However, this technique does not provide information about where sources of resilience or vulnerabilities may be located within the system which is equally important for managing. In order to locate sources of resilience and vulnerabilities it is necessary to map the inner workings of a system and track operational dynamics as performance measurements are collected. Hollnagel (2012) presented the functional resonance analysis method (FRAM), which is well suited to tracking operational dynamics of socio-technical systems. The FRAM maps operational activities and tracks variability in the outputs of those activities. The variability can provide a sense of the level of adaptation present in the operation. The FRAM also provides guidance about the types of relationships that may exist between activities, which can be especially useful for understanding relationships between human activities and activities done by technologies. Though the FRAM is useful for modelling dynamics of operations and improving the understanding of the systems inner workings, it does not provide a framework for quantification.

Returning to Arctic shipping safety, it can be reasoned that it is well-suited to adaptive safety approaches. Arctic shipping is a socio-technical system with many uncertainties. Humans play major roles in the outcome of the operation. In fact the main objective of the ship operator is to adjust the ship's conditions if needed to avoid hazards. Therefore, an appropriate way to investigate ship operations is to use the FRAM to track the inner workings of the operation, and use system performance measurement as a way to include quantification of performance.

1.3. Background Knowledge and Gaps

In safety and risk, there is a need to improve the knowledge base in all areas, but there are significant knowledge gaps involving human factors and in turn organizational factors, as organizational actions are performed by humans. The lack of understanding of human factors in many safety and risk methodologies has been attributed to the reductionist approach, a technique for acquiring and organizing knowledge (Vicente, 2004). The approach is based on reducing problems into their most elementary parts and studying them in relative isolation. The understanding of the collective parts could then be used to understand the whole problem. This approach has been widely used for scientific inquiry over the last several centuries and it has been very valuable to the knowledge that has been gained to date, allowing for the discovery of the atom and mapping of the human genome. Figure 1.2 shows the reductionist approach to knowledge acquisition.

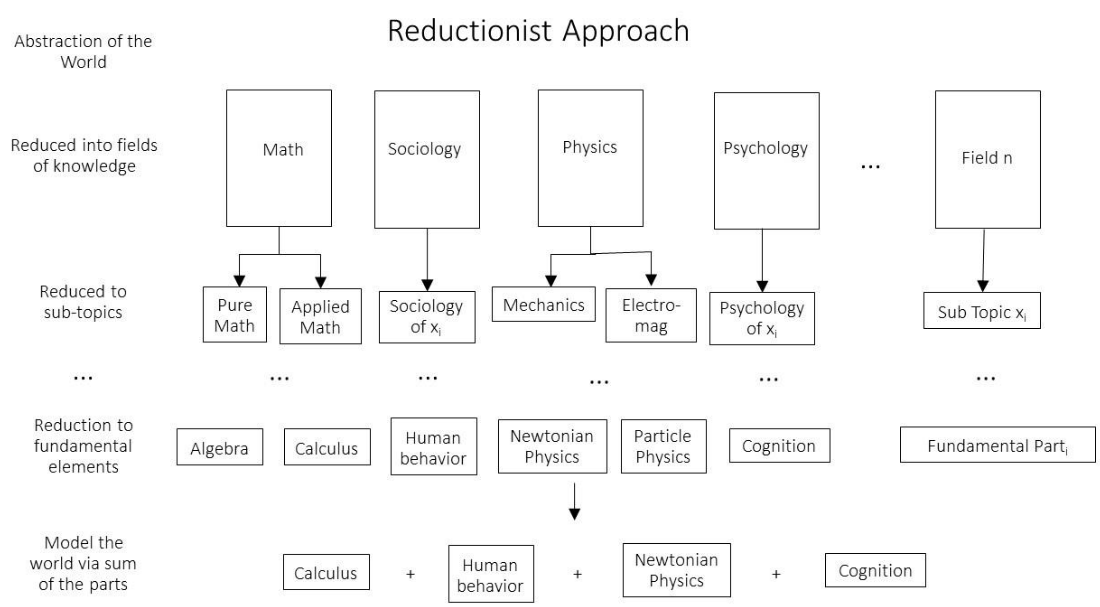


Figure 1.2: The reductionist approach to knowledge acquisition

Figure 1.2 illustrates that this approach produces knowledge that is largely divided by disciplinary boundaries. This allows for study at great depth within each discipline. The underlying assumption is that the scope of study can be reduced to the most fundamental parts and collective understandings can be obtained by combining the knowledge of the parts. This approach works well for obtaining collective understanding of linear systems as the whole can be understood as the sum of the parts, but leaves gaps in the collective knowledge base for non-linear systems. The reductionist approach also allows for more objective studies of knowledge to take place. As the scope of the problem is reduced, the number of influencing factors in that problem will be reduced, thus making it easier to perform “controlled” experiments, which allows for more objectivity. Despite the scientific knowledge gained using this approach, it has produced knowledge gaps in some areas that span multiple disciplines.

One of the most useful aspects of the reductionist approach is that it has allowed the advancers of knowledge to cope with complexity. Obtaining knowledge involves abstractions of observations from the world, which are combined with concepts that are created in our own minds. Also, because we are not purely observers, but also participants in the world we are studying, the complexity of relations between concepts and observations increases. Figure 1.3 depicts the complexity of knowledge abstraction, which the reductionist approach has helped us cope with through organization and reduction of scope.

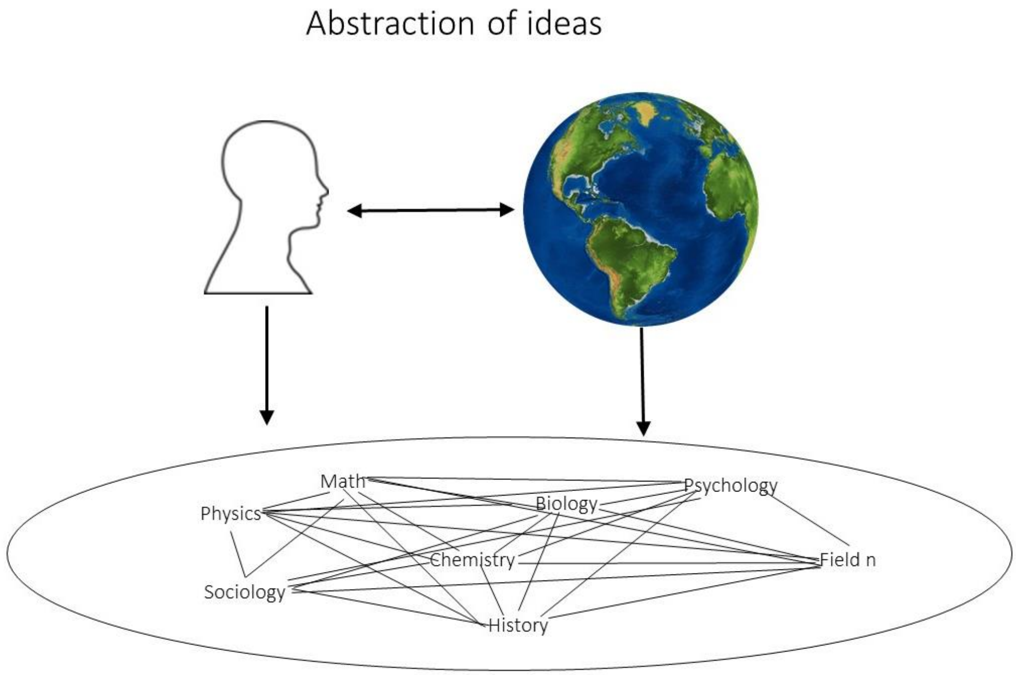


Figure 1.3: Complexity of knowledge abstraction

Another approach that can be used to cope with complexity is the holistic approach. This approach is different from the reductionist approach in that it focuses on understanding the relationships that exist between different elements and studies them as a whole. In the holistic approach, it may also be necessary to reduce the scope of study to manage complexity, but not to the level of the elementary parts. The scope may be reduced to a relatively small system initially, but could gradually become larger as relations and elements are understood. In order to produce collective knowledge in this approach, knowledge of individual studies must be synthesized. The process of synthesizing knowledge may not be as straightforward as simply combining the sum of the parts. Synthesis may require studies to be re-examined as a new whole to obtain collective knowledge. This process of using the holistic approach is shown in Figure 1.4.

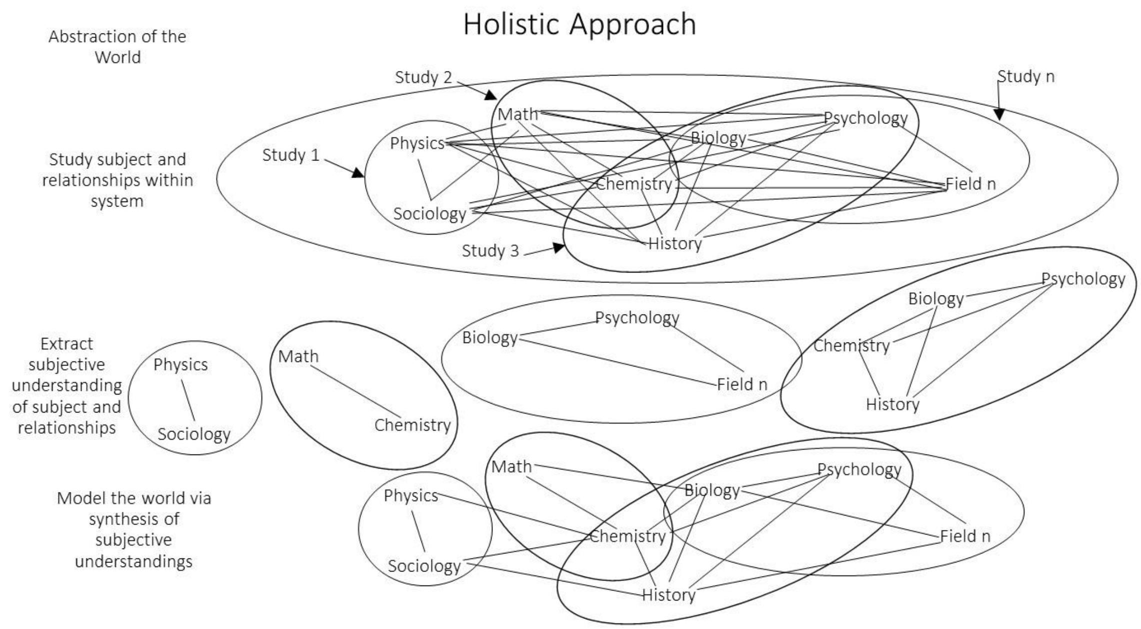


Figure 1.4: Holistic approach to knowledge acquisition

The holistic approach may also make it difficult to maintain objective understandings as it is difficult to isolate factors in this approach. In this approach, phenomena will be examined as they are experienced by observers. This can lead to subjective explanations of phenomena that contain biases arising from the way they were experienced. Synthesis can help provide more confidence to understandings that are obtained using this inherently biased approach. By synthesizing subjective understandings of the observed phenomena, there is an opportunity to check if the phenomena are seen in the same way across multiple studies. If the phenomena are observed in the same way after the studies have been synthesized, this will provide confidence that a consistent understanding of the phenomena has been obtained despite the biases.

Given the preceding discussion on reductionism and holism, it may lead to the question, which approach is better? There is no general answer to that question. Which method is the most appropriate will be largely determined by context. Reductionism and holism are paradigms that will shape the way the world is viewed, thus the way scientific inquiries are approached. Each approach may have value in certain contexts, and it may even show more value to use both approaches. However, since reductionism has been the preferred scientific approach for the last several centuries, there may be immediate knowledge gaps that can be addressed by using a holistic approach.

An emerging domain of knowledge over the past half century is complexity theory. Complexity theory is founded on the holistic paradigm and provides some structure to assessments of complex systems. Complexity theory is a composite of four other domains: 1) Self organization theory, 2) Non-linear systems theory, 3) Network theory, and 4) Adaptive systems theory (Colchester, 2016). This composite definition of complexity theory can be seen in Figure 1.5.

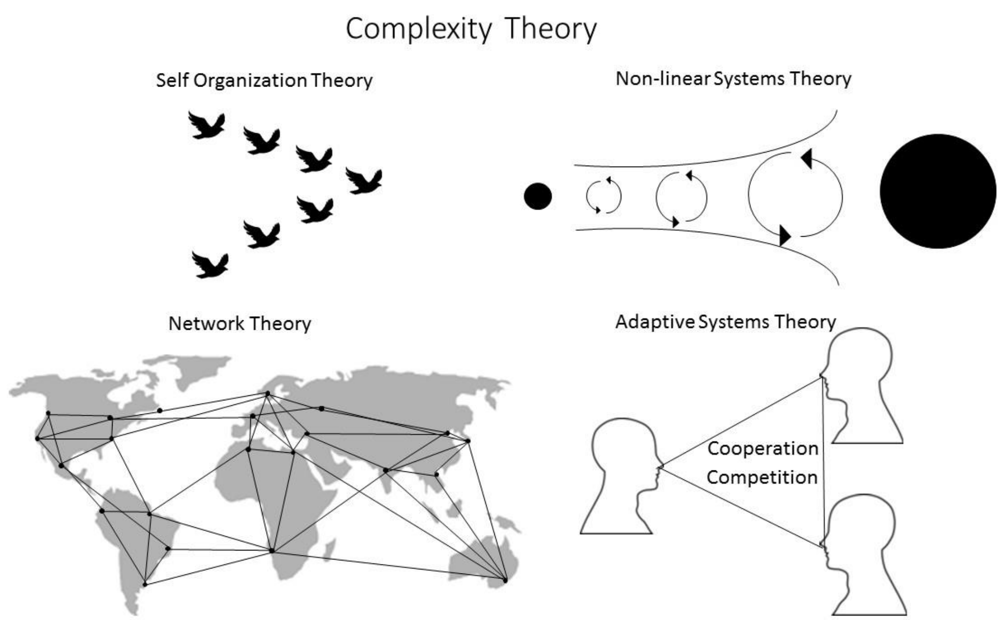


Figure 1.5: Composite definition of complexity theory

The four composite domains of complexity theory provide frameworks that can be used to understand characteristics of complex systems. These related domains can be described as follows:

- Self organization theory provides some understanding of how local interactions between system elements can bring about global organization patterns. For instance, interactions between individual birds can give rise to the “V shape” of the flock as they fly. There is no centralized coordination center responsible for this global phenomena of the flock: it is done by self organization among the individual birds. Another example may be how interactions between local businesses form global patterns of organization in regional, national, and international markets.
- Non-linear systems theory provides a basis to understand non-linear phenomena. Since linear systems have been defined previously as a system that can be represented by the sum of its parts, then a non-linear system is a system that can produce a whole that is different than the sum of its parts. For instance, adding bees and flowers to a garden or forest can produce changes that are much greater than the addition of flowers and bees.
- Network theory provides an understanding of connectivity between system elements. A global flight map would be an example of a network that represents connectivity between cities.
- Adaptive systems theory provides some basis to understand local adaptation within systems. Competition and/or coordination between local agents in systems can lead to changing conditions that require adaptations to maintain system functionality.

> This can be seen in our road transportation system, wherein agents make adaptation locally in roadways to either coordinate or compete for road space, which can produce a number of different outcomes.

Another common concept in scientific inquiry is causality. This search for cause and effect relationships has been a cornerstone for modelling the world we live in. However, causality manifests in different ways in linear systems and non-linear systems, as depicted in Figure 1.6. Linear causation is unidirectional, meaning that a cause will produce an effect but an effect will have no influence on a cause. This conception of causality has been effective for linear system modelling. Non-linear causality includes two way influence between cause and effect. The cause will influence an effect and the effect can then feedback to influence the cause. This process of non-linear causation might be difficult to imagine since we typically tend to imagine cause and effect relationships occurring sequentially. This is related to our linear conception of time. Consider the representation of non-linear causation with respect to time in Figure 1.6. This figure displays how we can project a future goal and that future goal can feedback to influence how we might act in the present. For example, when cooking a meal you might project what your meal will look like after it’s cooked to decide on the actions you will take to prepare it. The presence of feedback loop(s) creates non-linearity.

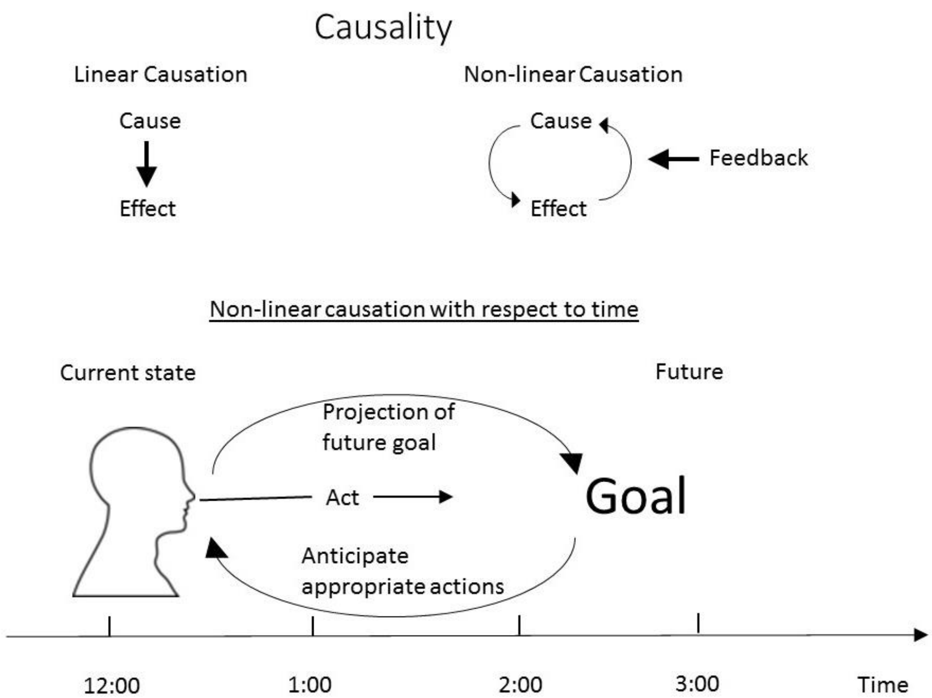


Figure 1.6: Linear and non-linear causality

Another concept that is present in complexity theory, and the holistic paradigm, is emergence. This concept is akin to causality in linear systems as it tries to provide reason to outcomes. Whereas outcomes can be thought to have occurred because of their causes in linear systems, in complex (non-linear) systems outcomes are thought to have occurred because of emergent patterns of organization between system elements. Emergence is a product of four properties in complex systems (Colchester, 2017): 1) Non-linearity, 2) Synergies, 3) Self organization, 4) Pattern formation. See the four properties of emergence in Figure 1.7.

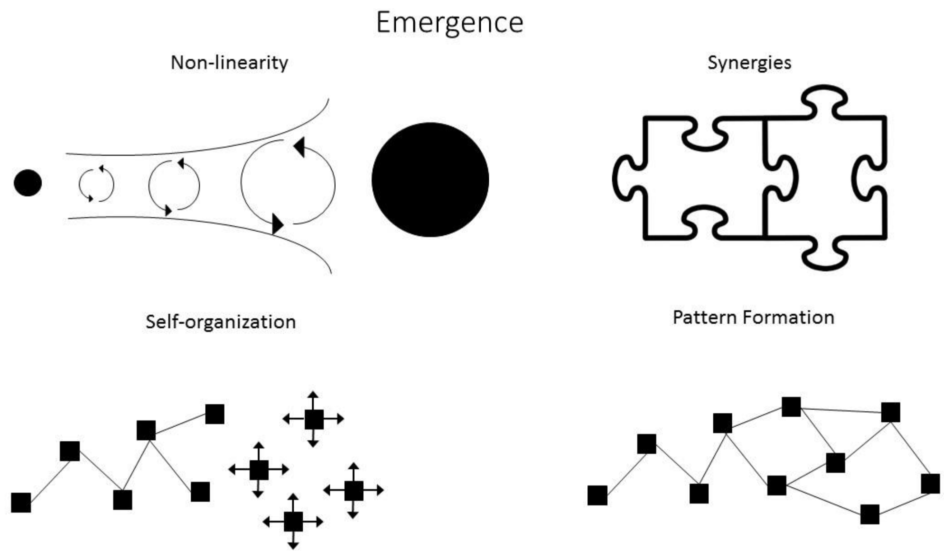


Figure 1.7: Four properties of emergence

Emergence can be influenced by feedback loops in non-linear systems. Multiple feedback processes have the potential to greatly amplify outcomes, to seem as if an unexpected outcome emerged from a modest set of initial conditions. Self-organization that occurs between local system elements can give rise to emergent outcomes of the system. As the local system elements self-organize, outcomes emerge from patterns of organization that are due to the combined effects of multi-element self-organization, making it difficult to determine any direct causal link to the outcome. Synergies between system elements play an important role in emergence. Synergies are the combined interactions between elements that produce a combined effect that do not equal the sum of the parts, see Figure 1.8. Two parameters responsible for synergies in systems are differentiation and integration. Differentiation is the component that allows for specialization and integration defines how specialized parts are configured to produce synergistic outcomes. Organizations have specialized workers who, when properly integrated, can produce outcomes greater than the same number of unspecialized, improperly integrated, people. The example in Figure 1.8 illustrates how a collection of specialized body parts when integrated properly can form a human. The same parts, when integrated differently, may not synergize to a human, but maybe another life form.

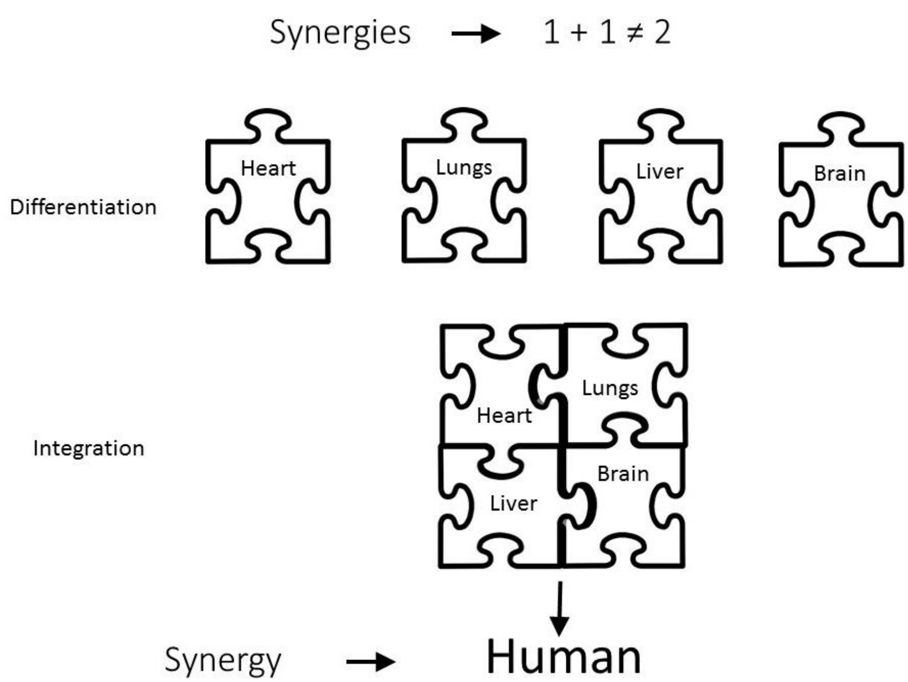


Figure 1.8: Illustration of synergies

Emergence can also be characterized on a spectrum ranging from weak to strong emergence (Figure 1.9). Weakly emergent phenomena are phenomena that are produced through synergistic interactions, without a linear causal explanation, but a causal relationship may be determined after that emergent phenomena is incorporated into a model. This form of emergence is called epistemological emergence. The phenomena seems emergent because it hasn't been experienced before. Weak emergence can describe unforeseen outcomes or surprises, but after they have been observed they can be incorporated into the epistemology. On the stronger end of the emergence spectrum there is ontological emergence. Ontological emergence is related to the nature of being, and in that sense the emergent phenomena just seems to occur without any (or very little) understanding of the mechanisms that would produce it. A common example of strong emergence is how consciousness emerges from the nervous system. There is a grey area between the distinction of epistemological emergence and ontological emergence. If new epistemology is obtained that provides an explanation for a phenomena that was once thought to be ontological, the strength of that emergent phenomena would decrease. Thus, one could ask was that emergent phenomena actually ontological in the first place. Regardless of the labels that are placed on emergent phenomena, one should have an appreciation for the range of strength for those emergent phenomena.

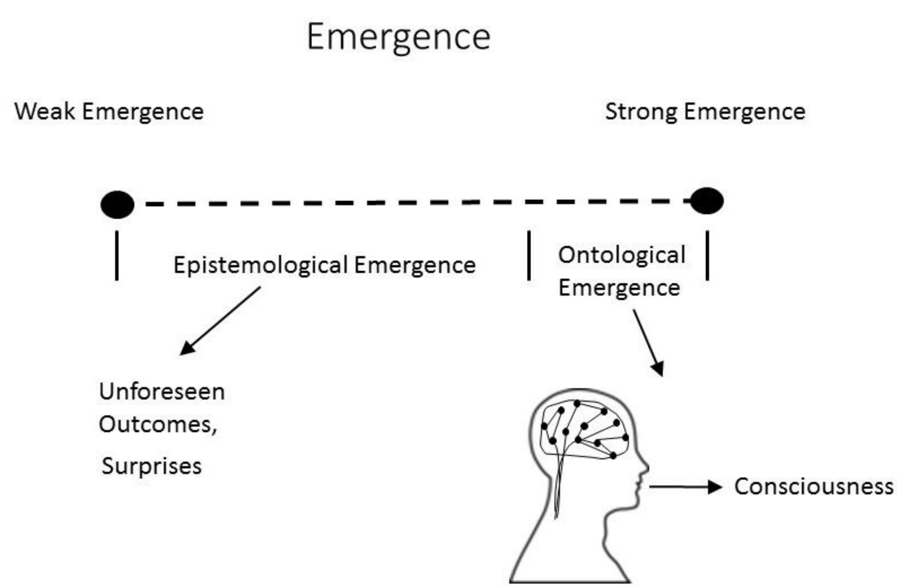


Figure 1.9: Strong and weak emergence

These concepts from complexity theory can help provide an understanding of what a complex system is (Colchester, 2016). A complex system is said to have four properties (Figure 1.10): Numerosity, Non-linearity, Connectivity, and adaptation. While these properties will vary from system to system, they may be used as measures of complexity.

- Numerosity: The number of elements in a system. A system with more elements may be seen as more complex.
- Non-linearity: A system's sensitivity to initial conditions. Non-linearity will be demonstrated when small changes in initial conditions produce disproportionally large changes in the system's outcomes. A system that exhibits this non-linear behavior is complex.
- Connectivity: Connectivity describes the relationships between the system elements. The number of connections between elements can be used as a measure of complexity, with more connections being more complex.
- Adaptation: Adaptation represents the system's ability to self-organize and make local adjustments to perturbations and maintain functionality. The number of potential/actual adjustments in a system may be seen as a measure of complexity.

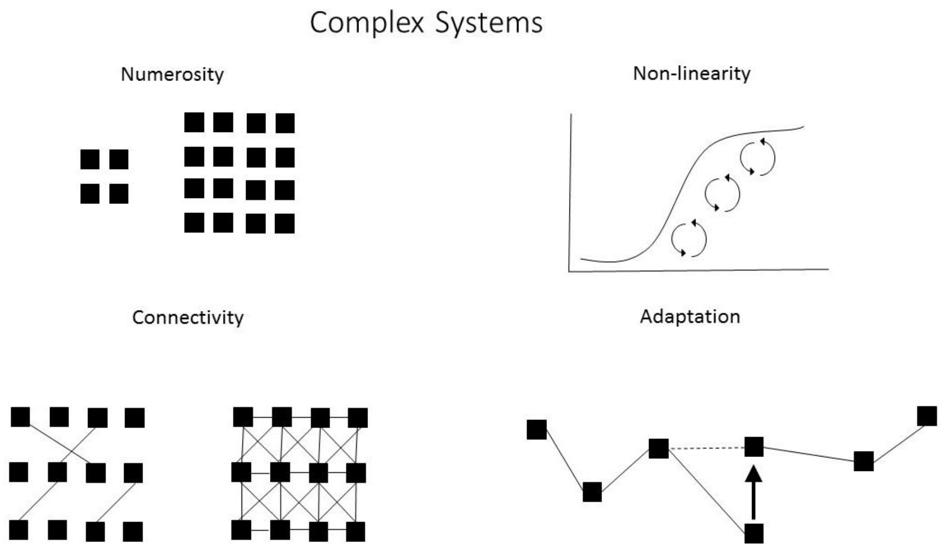


Figure 1.10: Defining a complex system

1.4. Safety and risk

The words safety and risk have often been used as antonyms, safety being used to describe everything that produces a good outcome, and risk to describe anything that produces a bad outcome. The dichotomy of this perspective can be seen as a by-product of the reductionist approach. Safety and risk have become divided disciplines. These very closely related topics have their own distinct bodies of knowledge and terminology. To further explain the fragmentation of knowledge, knowledge within these disciplines is largely divided into sub-topics of technological factors, human factors, and organizational factors. The reductionist approach has produced valuable specialized knowledge, but has left gaps in the collective knowledge pertaining to the relationships between sub-topics of safety and risk. There is potential to address these fundamental knowledge gaps in safety and risk by using a holistic approach.

The safety and risk domains have a plethora of tools that can be used to understand specific applications. This thesis is intended to make contributions to safety and risk in a way that would be applicable to Arctic shipping. Arctic shipping contains considerable involvement of technical, human and organization factors. These type of operations are called socio-technical systems. Moreover, Arctic shipping has many elements with high connectivity, non-linear behaviors, and many local adaptations so Arctic shipping can also be categorized as a complex socio-technical system. Thus, this characterization should provide the context for examining some of the available safety management approaches and selecting an appropriate one to investigate Arctic shipping.

Safety is important to all participants of an operation. Operations can span many different domains, thus there have been many different approaches to safety that are derived from the fundamentals of certain domains. This is consistent with the "siloed" knowledge bases of the reductionist method that is described in Figure 1.2. Engineering and other math-heavy sciences have been in favor of risk based approaches to safety, which typically allows for quantifiable analytics of operations. The quantifiable nature of analysis allows engineers to use familiar mathematical tools, which provides some comfort in adopting risk-based approaches. Quantification also provides a basis for objective analysis, which can help with model "validation" and can provide confidence about certain operational insights to help manage safety. The underlying philosophy of risk-based approaches is that safety will be improved by avoiding (or mitigating) risks. Other domains that are more comfortable with purely qualitative analysis, such as, psychology, kinesiology, and medicine, have made other contributions to safety, which are not necessarily consistent with risk-based approaches. These more qualitative approaches are based on the philosophy that safety can be improved by promoting safe practices, thus avoiding risks that one may not have even characterized in a quantitative approach. A main source of supportive evidence for these safety-based approaches is in high-reliability organizations (HRO's) (Klein, 1999; Weick & Sutcliffe, 2007). HROs are defined as organizations that are called into action in elevated risk situations and maintain an impressive safety record, such as firefighters, paramedics, and certain military applications. In these fields, they have very little control over the level of risk that they have to operate in, but their attention to safety has proven to be a significant contributor to their impressive safety records. The qualitative nature of these approaches has made it difficult to merge with conventional risk-based approaches which provides a sense of "validation" to support safety and business decisions. The word "validation" appears in quotations in the preceding discussion about risk-based and safety-based approaches. That is because what is typically referred to as validation may be more appropriately termed calibration. The process for developing a model to inform safety management is displayed in Figure 1.11. A model is built from information, events, and data of the past. The model is then checked using the data. If the models outputs are in close enough agreement to the data, the model will be accepted. Once the model has been accepted, it will then be used to make predictions of the future, and those predictions will be the basis for safety management decisions. In this sense, it may be more appropriate to think of the model as calibrated to make a prediction of the future that is similar to what has been seen in the past. While this assumption that the future will be like the past works some of the time, it is not true for all cases and can leave model users susceptible to surprises. Therefore, the model is not generally valid either, but only valid for the past cases that have been used to build, check, and accept the model. The term calibration implies that the results produced by the model will fall within the calibrated range and that there may be a need to re-calibrate the model from time to time.

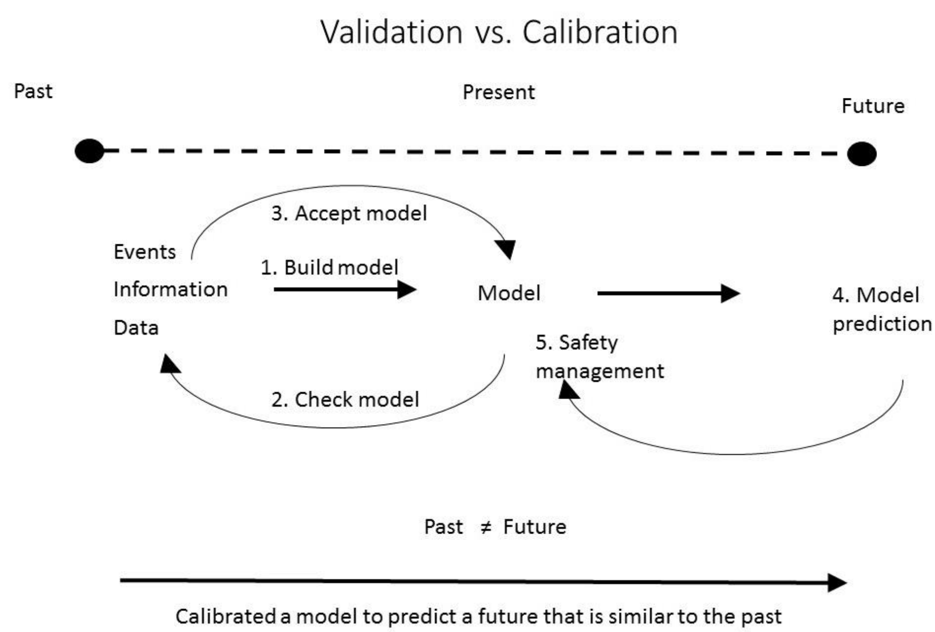


Figure 1.11: Model validation vs. calibration

In order to further understand some of the uncertainties that are inherently present in traditional risk-based approaches the "4 knowns" can be examined. The "4 knowns" is a popular knowledge characterization tool that is used in safety, risk, and project planning applications. The "4 knowns" state that knowledge can be characterized by 4 types of knowns: the known knowns, the known unknowns, the unknown knowns, and the unknown unknowns. The known knowns represent things that are known to be true, known unknowns represent things that are known to be not well understood, unknown knowns represent things that are believed to be known but are actually misunderstood, and unknown unknowns represent the things that have neither been thought of or observed before. This has been a useful tool to help remind decision makers about different forms of uncertainty that may exist in knowledge that is used to inform their decisions. However, this way of characterizing knowledge has epistemological flaws. Most notably, the characterization of known knowns implies that such knowledge is known with 100% certainty. From an epistemological perspective, knowledge can be thought of as beliefs of varying strength, where the strength varies in relation to evidence that supports that belief. While certain beliefs that have immense supporting evidence can be very strong, there will always be a possibility of observing contradictory evidence to that belief, thus preventing any knowledge from being 100% known. Figure 1.12 shows the 4 knowns as they pertain to the strength of belief perspective for knowledge characterization. Belief can exist on a spectrum of strength related to supporting evidence, existing somewhere between 0% to just less than 100%. Unknown unknowns can be characterized as 0% strength of belief because there has been no idea or observation yet to substantiate a belief. Known unknowns will typically be characterized as weak beliefs, as there is enough evidence to support the awareness of a phenomenon but not enough evidence to understand its mechanisms and interrelations. A grey area exists between unknown knowns and known knowns. While known knowns will typically be the most supported and strongest beliefs, unknown knowns will also be strong beliefs. Both are said to be known, thus implying a strong belief, but one is said to be true and the other a misunderstood truth. However, it will not be known if there is a misunderstanding of the knowledge until some evidence is observed that contradicts the prior belief. In order to counteract this inherent uncertainty of knowledge characterization, it is advantageous to constantly challenge your prior beliefs and continue to ensure that evidence is supporting them.

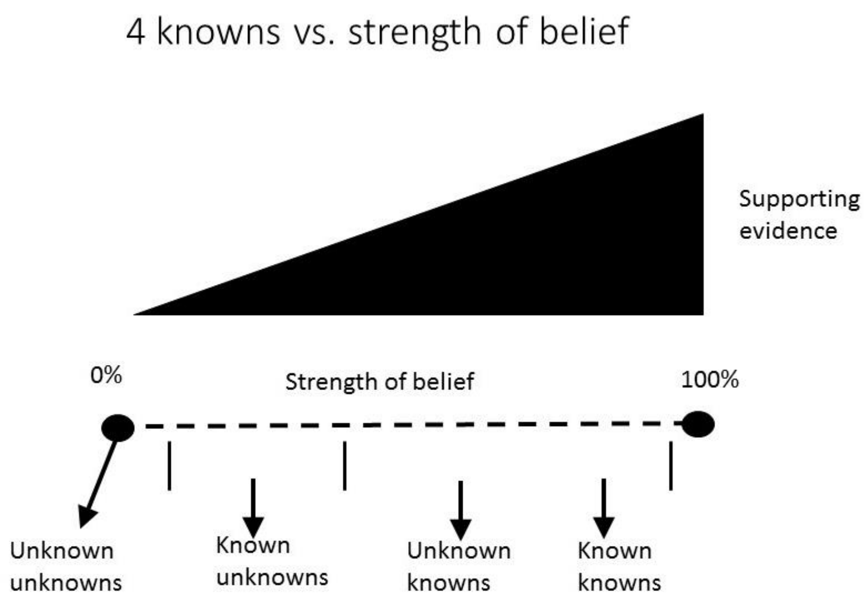


Figure 1.12: 4 knowns vs. strength of belief

Although both schools of thought - risk-based and safety-based approaches - have their own respective merits and shortcomings, the most effective approach will be to marry the two approaches. This movement has been seen in recent literature, under such names as Safety II and Safety Differently (Dekker, 2014; Hollnagel, 2014b). Both names are representative of a past where the go-to approach in safety and risk was to focus on accidents and try to prevent them. Safety II incorporates successful operations to build on the traditional accident focused approach, and claims to provide the most promise for improvement to safety going forward. Safety Differently, similarly suggests that safety has traditionally been approached through the study of accidents, but we should be thinking about safety differently, specifically by also studying successful operations. It is important to point out that these movements do not suggest that the ways of the past be forgotten, or that one approach should be chosen over the other. Rather, the way forward is to find ways to synthesize the two approaches to formulate the best understandings of industrial applications, which will help inform safety management of the future.

Safety II and Safety Differently are influenced by state-of-the-art understandings of human factors in industrial operations. Human factors have been and still are a major contributor to industrial accidents (Rothblum, 2000; Shappell & Wiegmann, 2004; U.S. Department of Energy, 2009). Traditional safety management strategies searched for “root causes” of accidents and then removed those causes. This strategy would often manifest as a human error being deemed responsible, resulting in removing the person responsible for the error, and replacing them with another person. While this use of personal accountability has the ability to shape human performance in a positive way in terms of safety, there are questions regarding the limits of positive change that can be enabled this way. By considering human factors in the context of how they influence accidents and successes, a different perspective is obtained. While operational adjustments made by humans can be seen as a contributor to accidents (and it is), when examining successful operations, it is observed that those adjustments also contribute significantly to success (Hollnagel, 2014b). Work in many industries is under-specified and outcomes can be difficult to foresee, thus those industries rely on operational adjustments to have success. Most of the time, those operational adjustments do result in success for the operation. The adjustment is made by the worker in real-time, with the best information available at that time, with the intentions of having a good outcome. From this perspective, when an operational adjustment made by a worker has a bad outcome, and then that person is replaced by another person to improve safety, it can be questioned whether this is the best way to improve safety in operations that rely so heavily on operational adjustments for success? The best way to improve safety for these types of operations is to understand the roles of the workers, how their actions might influence operational outcomes, and how they might be better supported to make the "correct" decisions more often.

This understanding of human factors aligns well with the concept of system safety. System safety is an approach that brings the system paradigm to safety. By thinking about industrial applications as systems of interconnected, non-linear process with local adjustments, it can change the way safety has traditionally been thought of. Figure 1.13 shows the implications of using the reductionist or system paradigm to view industrial operations. While the operation will remain constant regardless of the paradigm, the way it is seen will change. Each paradigm acts as a lens that the operation is viewed through, thus changing what is seen, and/or what is deemed important. By seeing the operation under a different paradigm, there is the potential to reshape old or form new safety concepts that will help inform future safety management knowledge.

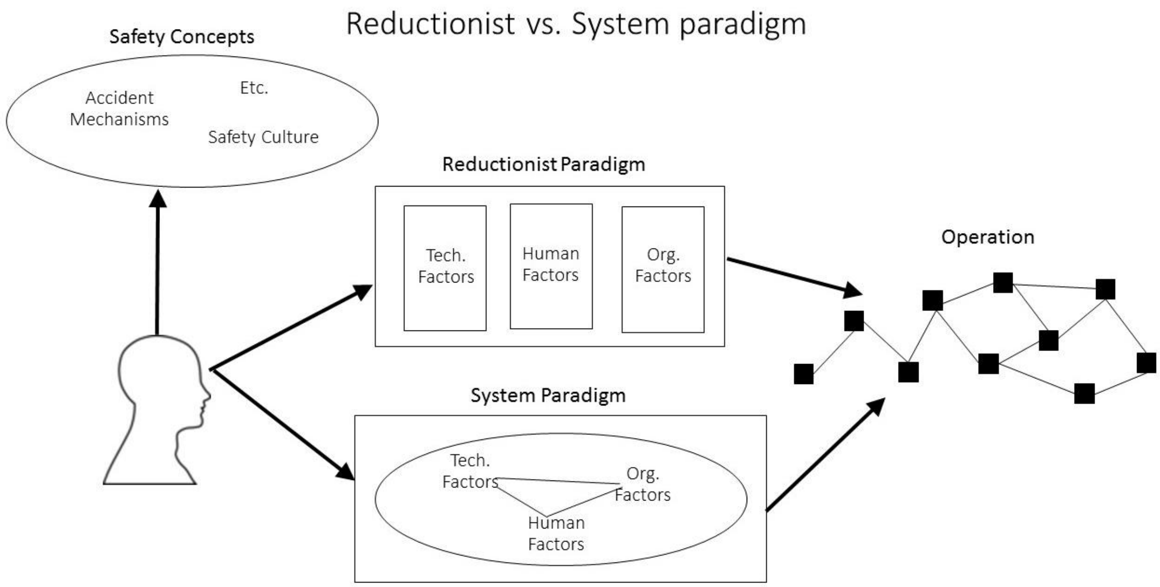


Figure 1.13: Reductionist vs. system paradigm for safety

The functional resonance analysis method (FRAM) is a method that uses the systems approach to understand functionality for sociotechnical systems. By using functionality, rather than error, as the lens to view operations through, new understandings of industrial safety can be obtained. Since functionality can be examined regardless of outcome, this method is in line with the Safety II approach. When studying functionality, the FRAM places emphasis on functions, their connectivity, variability, and local adaptations, which are believed to be the main sources for variable outcomes in sociotechnical operations under the FRAM paradigm. This paradigm provides a basis to reexamine safety concepts and update knowledge, if necessary, as seen in Figure 1.14.

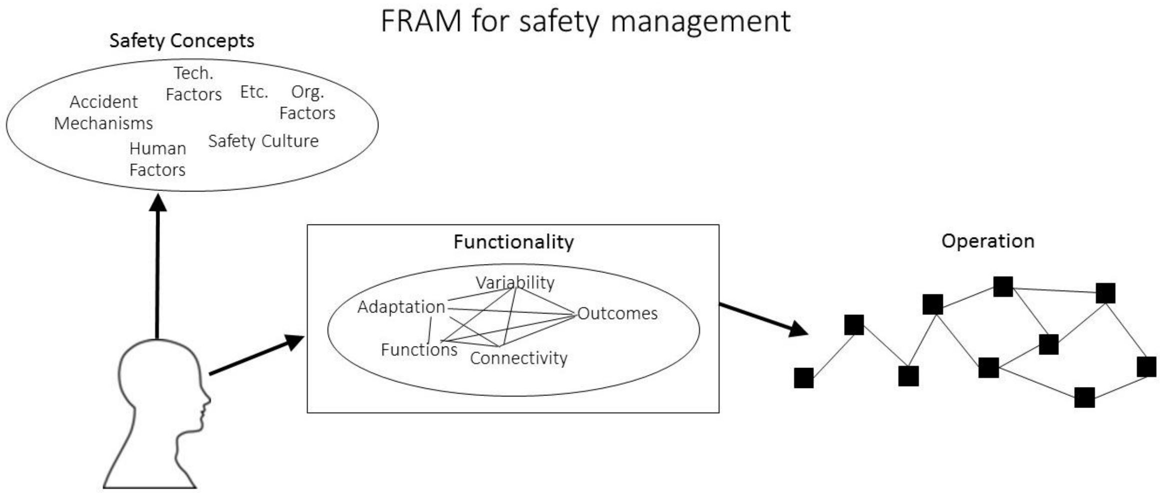


Figure 1.14: FRAM paradigm for safety management

Another concept that is in line with the Safety II approach is system resilience, resilience being the study of how systems persist in the face of adverse conditions. System performance measurement as a means to gauge resilience is of particular interest. This approach was presented by Ayyub (2014) and provides a framework for quantifying performance regardless of outcome, which is relevant to making comparisons of the outcomes. The framework suggests measuring the performance of a system over time as seen in Figure 1.15. The performance can be expressed, for example, as a percentage of the expected or desired performance for that system. There is no generic metric that can be used to measure system performance across different applications. The framework does, however, specify some suggested metrics for certain applications and advocates that suitable metrics should be representative of the main objective of the system being assessed.

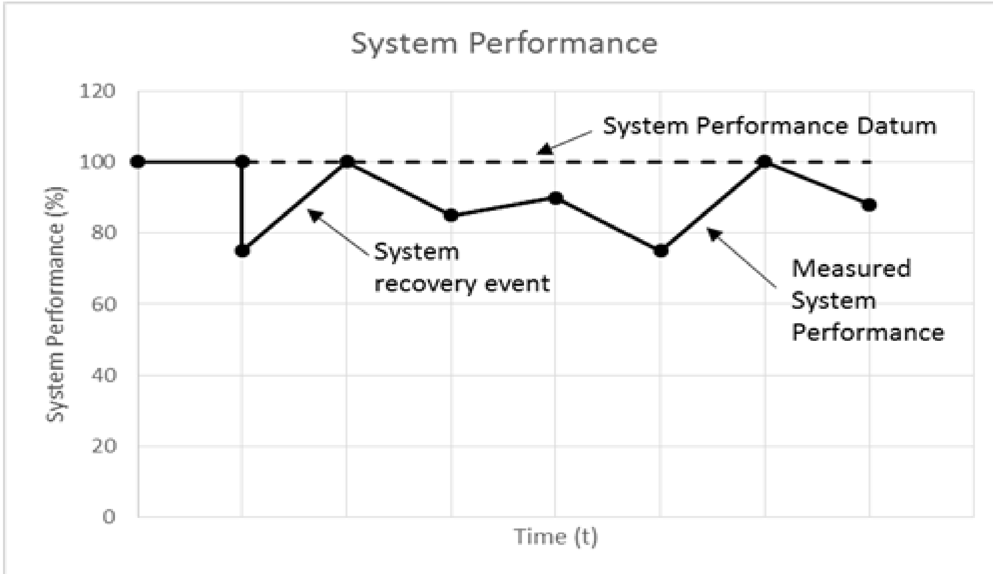


Figure 1.15: Measuring system performance over time (after Ayyub (2014))

1.5. Scope of work and contribution

This work provides contributions to safety research methodologies and insight to Arctic ship navigation safety. The contribution to safety research methods is from the creation of a performance measurement and process mapping/monitoring (PMPM) technique for safety management. The contribution to ship navigation safety is through the application of the PMPM method as it is developed throughout this thesis. This thesis is a manuscript style thesis, which consists of a collection of four manuscripts that appear as chapters 2, 3, 4, 5, respectively. The work in these manuscripts is described in the following.

Chapter 2 provides a state-of-the-art review of safety methods and philosophies with a comparison of three safety research tools: fault trees, Bayesian networks, and the FRAM. The comparison used a simple case study of a propane feed heater system to, as objectively as possible, compare the 3 methods. The conclusion from the comparison was that a best method could not be determined, but that each method provides different perspectives to the understanding of the same system. The choice of an appropriate method to investigate safety depends on the understandings that are desired by the user. Some highlights from the comparison study can be seen in Table 1.1.

Table 1.1: Comparison of the FT, BN, and FRAM methods

	Amount of information required	Type of information required	Accident explanation	Focus of investigation	Guided system description	Quantifiable
Fault Tree	lowest	components, logical relationships and individual failure data	Causal	Failure	No	Yes
Bayesian Network	more	components and CPT's	Causal	Failure	No	Yes
FRAM	most	Functions, functional interactions and variability	Emergent	Failure and success	Yes	No

Chapter 3 explores the development a FRAM model for Arctic ship navigation. A FRAM model for Arctic ship navigation was created by interviewing experienced ship navigators

(Figure 1.16). By probing the interviewees on the functionality (functions and variability) of ship navigation, insight was gained about the ship navigation processes and variations of it. From this insight, a FRAM model was created for Arctic ship navigation. This model provides a generic map of the connectivity of the processes involved for ship navigation, as informed by the interviewees. The model was then used to observe the functionality of the Exxon Valdez Grounding case study. This case study represented one variation of Arctic ship navigation and it was observed that the functional activity of this case was indeed dynamic. The analysis of this case study was the origin of the concept of functional signatures that are presented in the subsequent chapters. The insight that functional activity seen prior to the Exxon Valdez grounding could be likened to a signature that was left behind by that event. It would be interesting to see if other voyages of the Exxon Valdez had similar or different functional signatures at other times that it navigated the Valdez narrows, but this could not be done. The available data for the Exxon Valdez over its lifetime is reflective of the Safety I approach, in that it is focused only on the accident, and no information was documented about the many successful voyages through the same waterways.

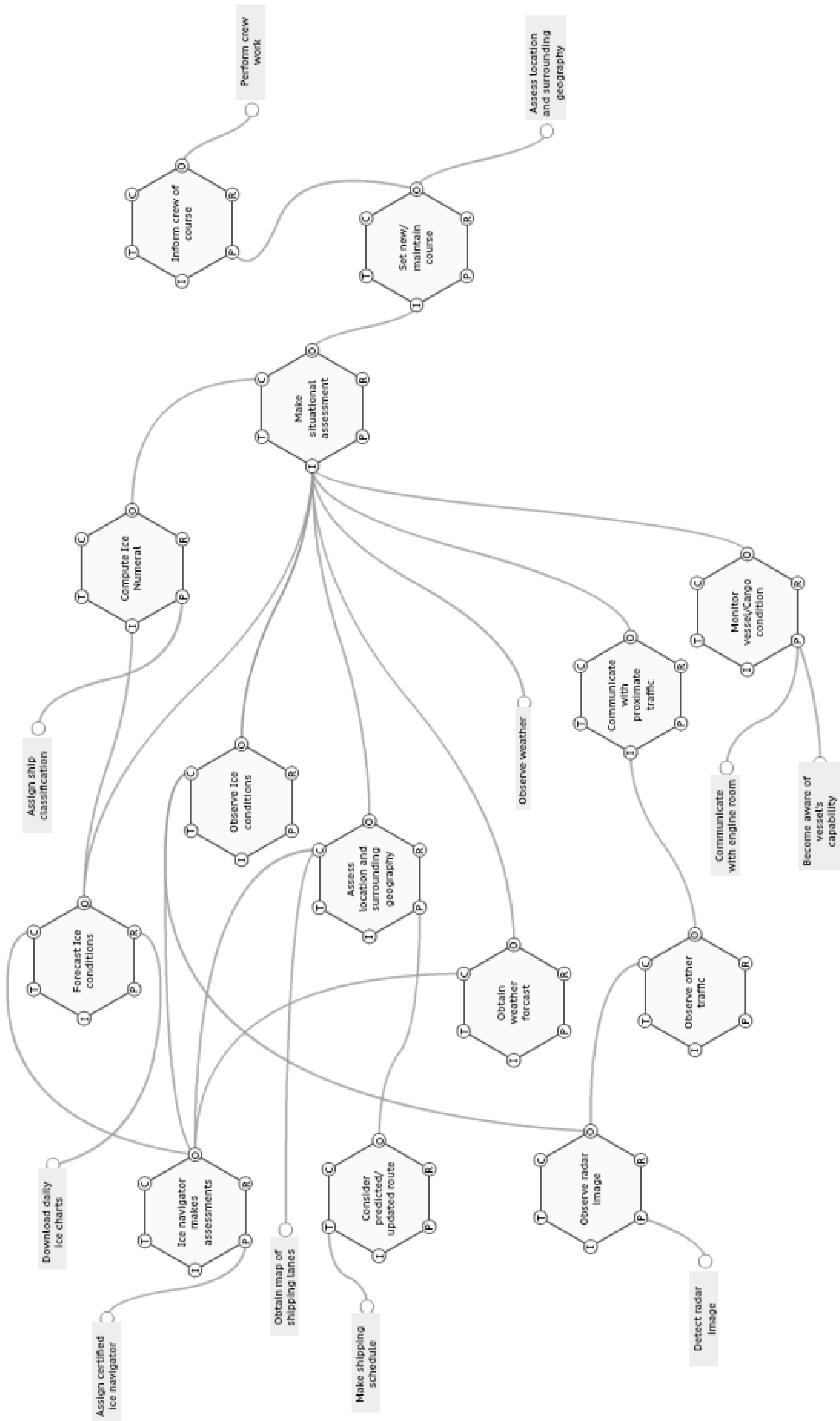


Figure 1.16: FRAM model for ship navigation with input from ship navigators

Chapter 4 presents the theoretical framework for the PMPM method. Using FRAM as described by Hollnagel (2012) allows for process mapping to be done through the creation of a FRAM model. The additional concept of functional signatures then enables processes to be monitored more thoroughly than with the standard procedures of the FRAM (Figure 1.17). The active functions at any time (t) are presented in bold red and the specific outputs of those functions at time (t) are written on the line coupling that output to its downstream function. The functional activity and functional outputs will vary over time, allowing users to more closely observe the functional dynamics of an operation. The functional activity for the operation can be monitored on a case by case basis. The concept of performance measurement is adopted from Ayyub (2014) to add a quantitative element to the FRAM that did not exist previously (Figure 1.15). The PMPM method is then demonstrated using a hypothetical case of driving a car to work.

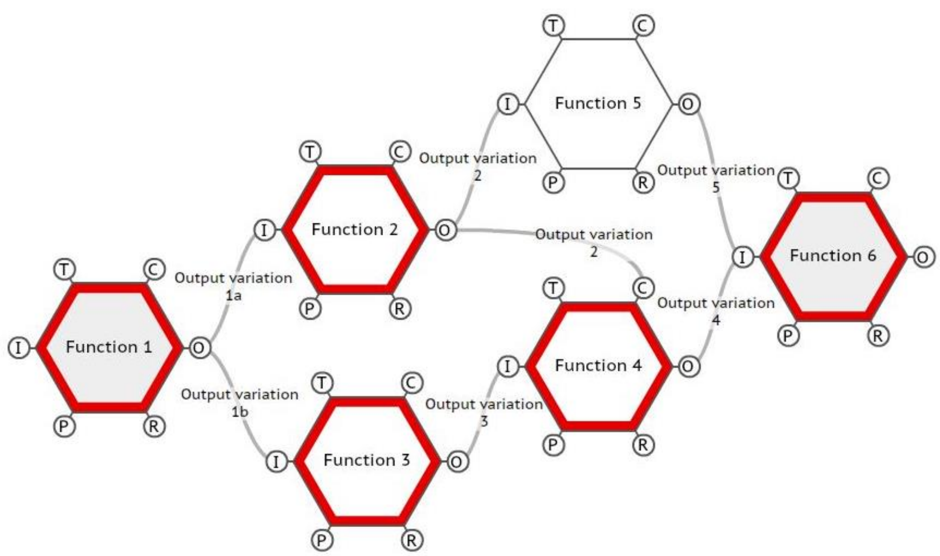


Figure 1.17: A functional signature for a given time (t)

Chapter 5 focuses on the application of the PMPM method. In this work, data is used from an ice management experiment in a ship simulator (Veitch et al., 2018). The application of the method helps to strengthen confidence in the practicalities of the method. This work also explored the statistics of functional signatures. The methodology can be seen in Figure 1.18. Additionally, the ship simulator data was acquired from an experiment where ship captains and cadets were asked to perform ice management operations using a simulated ship environment. The use of this data required approval from the tri-council ethics board for secondary use of data. See appendix A for ethics documentation.

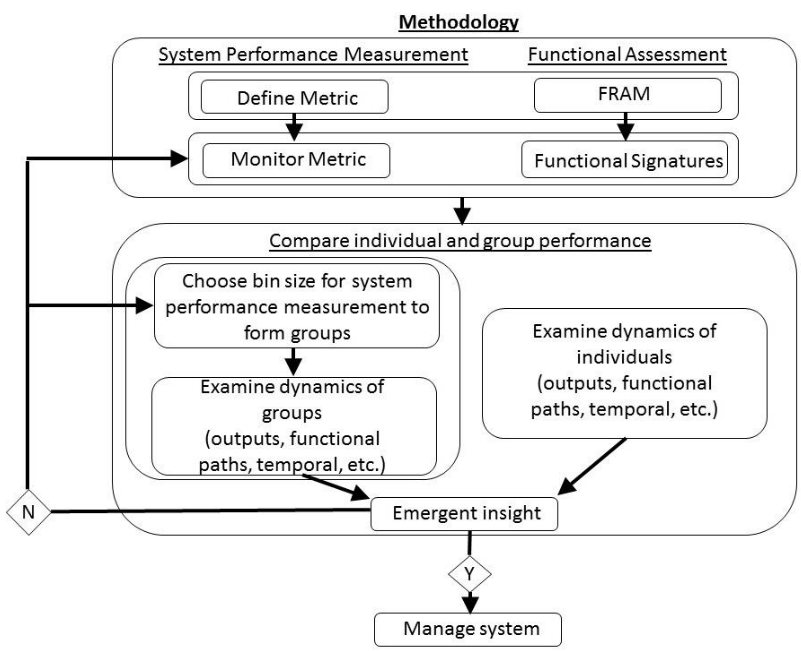


Figure 1.18: Flow chart of PMPMM methodology

The aggregate of this work forms the basis of the PMPM method with applications to Arctic ship navigation. Figure 1.19 displays the component parts of the method. The method has quantitative elements through the performance measurement component. This component helps understand the range of performance that is being achieved by the operation by measuring the overall performance of the operation. However, this measurement alone does not provide insight as to why higher or lower performance is being achieved. By coupling this measurement with functional signatures (process monitoring), there is potential to uncover why higher or lower performance is being achieved in any given case. If certain functional patterns can be identified as contributors to high or low performance, that insight can be used to manage the operation accordingly.

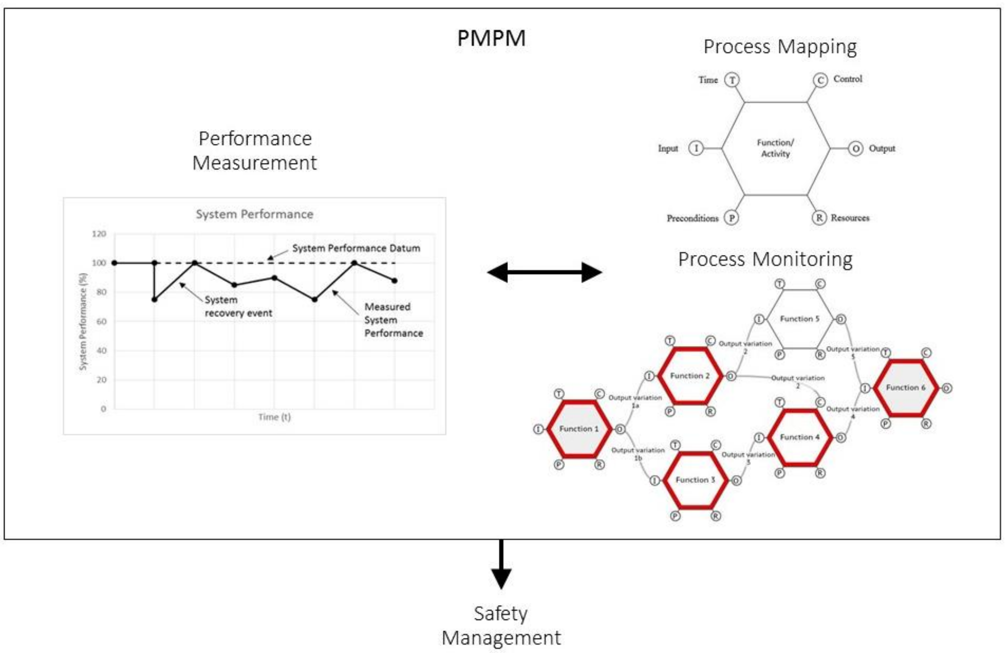


Figure 1.19: Components of PMPMM method for safety management

1.6. Organization of the thesis

The thesis is written in manuscript format, including four journal papers as chapters. Table 1.2 shows the papers written during the course of this research and establishes their connection to the overall objectives and associated tasks.

Table 1.2: Organization of manuscript thesis

Paper title	Research objective	Associated task
Chapter 2: Understanding industrial safety: comparing fault trees, Bayesian networks, and FRAM approaches	• To understand the evolution of safety methodologies • To improve the understanding and utility of fault trees, Bayesian networks and FRAM	• Review industrial safety • Comparison of fault tree, Bayesian network, and FRAM using a propane feed heater system • Discussion of the outcomes for each method
Chapter 3: Using FRAM to understand Arctic ship navigation: assessing work processes during the Exxon Valdez grounding	• To build a FRAM model for Arctic ship navigation • To illustrate the model’s utility by examining the functionality during the Exxon Valdez grounding	• Build a conceptual model for Arctic ship navigation • Discuss functionality with ship captains to improve conceptual model • Introduce the concept of functional signatures • Demonstrate functional signatures using the Exxon Valdez grounding
Chapter 4: Integration of resilience and FRAM for safety management	• To integrate resilience concepts with FRAM for safety management	• Present system performance measurement as a way to quantify success/failure

	• To discuss how the method might be used to manage safety	• Connect functional signatures to system performance measurement
Chapter 5: Visualizing and understanding the operational dynamics of a shipping operation	• To further develop functional signatures as a method to visualize operational dynamics • To present the application of this semi-quantitative method using data from an ice management simulator	• Present functional signatures to show the dynamics of the operation • Demonstrate the post-processing of data from the ice management simulator experiment • Perform data analysis using the semi-quantitative approach • Discuss this methods relevance to safety management

1.7. References

Arctic Council. (2009). *Arctic Marine Shipping Assessment 2009 Report*.

Aven, T., Andersen, H. B., Cox, T., Droguett, E. L., Greenberg, M., Guikema, S., … Zio, E. (2015). Risk Analysis Foundations. *Society for Risk Analysis*.

Ayyub, B. M. (2014). Systems resilience for multihazard environments: definition, metrics, and valuation for decision making. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, *34*(2), 340–355. https://doi.org/10.1111/risa.12093

Borys, D., Else, D., & Leggett, S. (2009). The fifth age of safety: the adaptive age. *Journal of Health & Safety Research & Practice*, *1*(1). Retrieved from http://chisholm.trainingvc.com.au/pluginfile.php/273772/course/section/28762/Journal%20article%20on%20adaptive%20age%20JHSRP_1-1_Borys_p19-27.pdf

Colchester, J. (2016). *Complexity Theory*. Retrieved from http://complexitylabs.io/complexity-theory-ebook/

Colchester, J. (2017). *Emergence Theory*. Retrieved from http://complexitylabs.io/emergence-theory-book/

Dekker, S. (2014). Safety Differently: Human Factors for a New Era, Second Edition. CRC Press.

Glendon, A. I., Clarke, S., & McKenna, E. (2006). *Human Safety and Risk Management* (Second Edition). Boca Raton, FL: CRC Press.

Hale, A. R., & Hovden, J. (1998). Management and culture: the third age of safety. A review of approaches to organizational aspects of safety, health and environment. In *Occupational Injury*. London: Taylor and Francis.

Hollnagel, E. (2012). *FRAM: The Functional Resonance Analysis Method*. Ashgate Publishing Ltd.

Hollnagel, E. (2014a). Is safety a subject for science? *Safety Science*, *67*, 21–24. https://doi.org/10.1016/j.ssci.2013.07.025

Hollnagel, E. (2014b). *Safety-I and Safety-II: The Past and Future of Safety Management* (1st ed.). Farnham, Surrey, UK England ; Burlington, VT, USA: Ashgate Publishing Ltd.

Klein, G. A. (1999). *Sources of Power: How People Make Decisions* (1 edition). Cambridge, Mass.: The MIT Press.

Marchenko, N. A. (2015). Ship Traffic in Svalbard Area and Safety Issues. Presented at the Port and Ocean Engineering under Arctic Conditions, Trondheim, Norway.

Moore, G. W. K., Schweiger, A., Zhang, J., & Steele, M. (2018). Collapse of the 2017 Winter Beaufort High: A Response to Thinning Sea Ice? *Geophysical Research Letters*, *45*(6), 2860–2869. https://doi.org/10.1002/2017GL076446

Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technologies*. Princeton, N.J: Princeton University Press.

Petty, A. A., Stroeve, J. C., Holland, P. R., Boisvert, L. N., Bliss, A. C., Kimura, N., & Meier, W. N. (2018). The Arctic sea ice cover of 2016: a year of record-low highs and higher-than-expected lows. *The Cryosphere*, *12*(2), 433–452. https://doi.org/10.5194/tc-12-433-2018

Petty, Alek A. (2018). A Possible Link Between Winter Arctic Sea Ice Decline and a Collapse of the Beaufort High? *Geophysical Research Letters*, *45*(6), 2879–2882. https://doi.org/10.1002/2018GL077704

Rothblum, A. M. (2000). Human Error and Marine Safety. Presented at the National Safety Council Congress and Expo, Orlando, USA.

Shappell, S., & Wiegmann, D. (2004). HFACS Analysis of Military and Civilian Aviation Accidents: A North American Comparison. Presented at the ISASI Seminar, Gold Coast, Austrailia.

U.S. Department of Energy. (2009). *Human Performance Improvement Handbook - Volume 1: Concepts and Principles* (No. DOE-HDBK-1028-2009). Washington, D.C.

Veitch, E., Molyneux, D., Smith, J., & Veitch, B. (2018). Investigating the influence of bridge officer experience on ice management effectiveness using a marine simulator experiment. *Journal of Offshore Mechanics and Arctic Engineering*. https://doi.org/10.1115/1.4041761

Vicente, K. (2004). The Human Factor: Revolutionizing the Way People Live with Technology. New York: Routledge.

Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the Unexpected: Resilient Performance in an Age of Uncertainty* (2 edition). San Francisco: Jossey-Bass.

2. UNDERSTANDING INDUSTRIAL SAFETY: COMPARING FAULT TREE, BAYESIAN NETWORK, AND FRAM APPROACHES

2.1. Co-authorship statement

A version of this manuscript has been accepted for publication in the Journal of loss prevention in the process industries, written by authors, Doug Smith, Brian Veitch, Faisal Khan, and Rocky Taylor. Author Doug Smith led the writing of this review paper including, the literature review, case study and discussion. All authors participated in discussions that helped enhance the concepts presented in the discussion section of this paper. All authors revised, edited, and made recommendations for improvements to earlier drafts of this paper.

2.2. Abstract

Industrial accidents are a major concern for companies and families alike. It is a high priority to all stakeholders that steps be taken to prevent accidents from occurring. In this paper, three approaches to safety are examined: fault trees (FT), Bayesian networks (BN), and the Functional Resonance Analysis Method (FRAM). A case study of a propane feed control system is used to apply these methods. In order to make safety improvements to industrial workplaces high understanding of the systems is required. It is shown that consideration of the chance of failure of the system components, as in the FT and BN approaches, may not provide enough understanding to fully inform safety assessments. The

FT and BN methods are top-down approaches that are formed from the perspective of management in workplaces. The FRAM methodology uses a bottom-up approach from the operational perspective to improve the understanding of the industrial workplace. The FRAM approach can provide added insight to the human factor and context and increase the rate at which we learn by considering successes as well as failures. FRAM can be a valuable tool for industrial safety assessment and to consider industrial safety holistically, by providing a framework to examine the operations in detail. However, operations should be considered using both top-down and bottom-up perspectives and all operational experience to make the most informed safety decisions.

2.3. Introduction

Understanding industrial accidents will always be at the forefront of industrial safety assessments. This understanding provides the information necessary to apply accident preventative measures to industrial processes. It is unlikely that complete understanding will ever be achieved, given the continual evolution of workplaces. With constantly evolving technologies and societal values, accident theories must also evolve to reflect the current state of knowledge. It is important to understand the evolution of industrial safety assessments and how they are influenced by technologies, societal values, and history.

Societal values are often reflected by the actions of governments and societal leaders. The Code of Hammurabi (Circa 1750 B.C.) is one of the earliest extant codes reflecting the laws of 18th century BC Mesopotamia. This document describes some 300 laws that should be enforced, including “appropriate” punishments for worker malpractice or early industrial accidents. The code was largely based on the retribution principle and also prescribes punishment by the societal level of the victim. This type of legislation would be completely inadequate in today's societies, although it provided some sense of accountability against negligence. The code violates today's standards of human rights, but does reflect what was acceptable in one of the most influential civilizations of the time. This effort to shape human behavior is cited as an early document that addressed health and safety (Speegle, 2012).

Societies have evolved a great deal since then, creating industries which in turn brought about industrial safety assessments. During the industrial revolution, workplaces started to resemble what is seen in today's industries. Safety was approached at that time by using science and engineering to design technologies. Improvements in safety were achieved by adapting first principles and technological advancements to existing systems. An early example of this is the Railroad Safety Appliance Act of 1893 (Hollnagel, 2014b). This act was formed because of public outcry in response to the many casualties of railway work at the time (Louisell & Anderson, 1953). The US government implemented the Railroad Safety Appliance Act to legislate the use of technological advancements, such as air brakes and automatic car couplers, on American railroads. This would reduce the number of injuries to, and fatalities of, railway workers by eliminating manual car coupling. This combination of technological advancement and societal pressures resulted in one of the most significant documents with respect to industrial safety.

In 1979, the Three Mile Island Nuclear Power plant suffered a partial meltdown. A valve that was stuck open in the water cooling system for the secondary core was leaking the cooling water. When control room operators noticed warning lights, the possibility of water cooling failure was dismissed because normal water pressure was measured upstream of the leak. A series of actions was taken to deescalate the situation, but all failed due to improper assessment (US Nuclear Regulatory Commission, 2013). This accident changed the way we understand accidents. Retrospective Analysis uncovered a missing element in accident analysis and human factors became an integral part of formal safety assessments thereafter. Shortly after, the US Nuclear Regulatory Commission published a handbook on Human Reliability (Swain & Guttman, 1983).

In 1986, two accidents occurred that brought attention to another element that was missing in safety assessments. On January 28, 1986, the Challenger space shuttle exploded during its take off, resulting in the loss of life of the six astronauts and one school teacher onboard. While there is consensus that the explosion resulted from an O-ring failure, the subsequent investigation would reveal many questions about the understanding of the risks by the shuttle's management team (Feynman, 1999). On April 26, 1986, the explosion of reactor 4 at the Chernobyl nuclear power plant devastated the area with effects that are still being felt today. Again this accident brought attention to the human factor, but also to the organization's role in human reliability assessments (Meshkati, 1991). It was seen from these accidents that organizations can shape human behavior, and their role has since been considered in formal safety assessments.

History, technology and societal values have shaped our current understanding of industrial accidents. Modern safety assessments require consideration of technological, human and organizational factors, which represent the so-called, socio-technological system. This evolution of safety assessments is a direct result of learning from past accidents in evolving industries and societies. As we learn from accidents retroactively, there is lag between the rates at which industries evolve and safety assessments evolve: Is there a way to reduce this lag time and perform safety assessments that are more representative of the current states of the industries? In this paper, we compare how modern accident analysis techniques process information of industrial workplaces, using a propane feed control system as an example, and examine how that relates to the current understanding of accident processes and industrial operations.

2.4. Background

Much as safety policy has evolved, so too has the background knowledge that influence safety methodologies. This has been described in terms of the ages of safety, respectively: The age of technology, the age of human factors, and the age of safety management (Hale & Hovden, 1998). Each age is characterized by the consideration of a new class of factors that are revealed as important as past accidents are studied. The age of technology refers to safety assessments that are approached by consideration of technical factors. The age of the human factor refers to the adoption of the human element in safety assessments. The age of safety management refers to incorporation of organizational factors and understanding how organizations can shape human behavior. It has been stated that there has been another age of safety since, the age of integration (Glendon et al., 2006). This age is defined by the integration of the previous three ages into more holistic accident models. There is now a movement to bring about a new age of safety, the adaptive age (Borys et al., 2009). This age refers to the use of systemic accident theories to produce adaptive safety systems. The current age of safety is somewhere between the age of integration and the adaptive age, with practitioners lagging behind researchers and academics (Underwood & Waterson, 2013).

The age of integration is a natural progression of the past principles that have been adopted from risk analysis and reliability engineering. Reliability engineering built a framework that has been quite successful in describing and understanding technical factors. Failure rates of technical components are used to form reliability assessments, and causal relationships are studied for said technologies. The failure rates can then be translated to failure probabilities and used in risk assessments and cost-benefit analysis. This methodology extended into the age of human factors and age of safety management. This produced human reliability assessments. Methods such as THERP (Swain, 1963), ATHEANA (Cooper et al., 1996), CREAM (Hollnagel, 1998) and HEPI (Khan, Amyotte, & DiMattia, 2006) have been developed to predict human error. Predicting human failure probabilities allowed the human element to be adopted in the risk framework. There is more to consider when examining accidents than technical, human and organizational factors. There are also extreme weather events, political situations, harsh environments, and unexpected deviations from normal operations. These are external factors that cannot be controlled by the stakeholders of the operation, although they must be managed. This has led to the use of Bayesian Networks as a tool to incorporate these complexly interrelated factors into probabilistic models that are updatable and allow the accident risk to be quantified.

The adaptive age of safety, while still building on the information from past ages, requires a shift in the way we view accidents. Accidents are not viewed as resultant of direct causes, but rather as emergent from system variability or from gaps in system control. This is an important distinction because many of the system components that are labeled causes are also present during successful operations. Appropriate actions can be easy to prescribe after the outcome is known, but outcomes are not known in advance. When considering the human factor, emergent accident theories are appropriate because actions cannot be prescribed for all possible conditions found in modern workplaces. This perspective leads to the realization that accident scenarios are not completely preventable and predictable, which makes sense given the continual evolution of industrial workplaces. In the adaptive age, focus is placed on designing safety systems that are adaptable and resilient against emergent accident scenarios.

To examine the difference between the integrative and adaptive age, the following section will examine the case of a propane feed control system. The safety of the system will be examined first by probabilistic approaches: Fault Tree (FT) and Bayesian Network (BN). The system safety will then be examined using an adaptive accident model, the Functional Resonance Analysis Method (FRAM).

2.4.1. FRAM

FRAM is a systemic accident analysis method that is developed from the fundamentals of resilience engineering (Hollnagel, Woods, & Leveson, 2006). Resilience engineering is the study of why systems or objects work in the face of adversity, and also how to achieve robust and flexible designs that will work even when faced with unfavorable conditions. As socio-technological systems are often under-specified, lack comprehensive understanding, and contain inherent performance variations, it is then appropriate to use such a systemic approach. FRAM can be used to achieve safety and understand how the system may be able to maintain a safe state even when subjected to dynamic operational conditions.

FRAM is based on four underlying principles (Hollnagel, 2012):

- Failures and successes are equivalent in the way that they happen for the same reason. Alternatively, it can be said that things go wrong for the same reasons that they go right.
- Daily performance of socio-technical systems, including humans individually and collectively, is always adjusted to match the system conditions.
- Many of the outcomes of the system that we notice, and also the ones we don't notice, are emergent rather than resultant.
- Relations and dependencies must be described as they develop in a particular situation and not as cause-effect links. This is done through functional resonance.

Traditional safety analysis methods have focused on failures and treated them as a cause and effect relationship. The cause is often viewed as a deviation from a prescribed procedure. It is impossible to prescribe procedures that are adequate for all conditions in a dynamic system. Adjustment or deviations are necessary for successes as well. The adaptive interaction between humans and technology is essential to operations, and labels such as successes and failures can only be determined after the outcomes are known.

If it is accepted that successes and failures happen for the same reason, then the outcomes are emergent and not resultant. The outcome emerges from variations in the functions of the system and outcomes might only be noticed when the variable system performance rises above the detection threshold. The variable system performance can be thought of as a combination of weak signals that interact in such a way that may produce an amplified performance variability for the overall system. This concept is similar to stochastic resonance, where random noise is added to a weak signal and the interaction will result in resonance and the previously undetectable weak signal will then be detectable (Hollnagel, 2012). In a socio-technological system, the noise is not random but rather the mixed signals from the other interacting system functions. The combined interaction of variable functional outputs from the individual system function can produce functional resonance. The result will be a noticeable variation in overall system performance.

FRAM is a novel method for assessment of safety using a holistic approach. The method describes the functions (what you do) that are necessary to make a system operate. The functions have 6 parameters that couple the system function (Figure 2.1). It addresses ways of coping with the complexities of socio-technological systems in an easily understandable way.

There are 4 steps to conducting a FRAM analysis (Hollnagel, 2012). The first step is to identify and describe the functions necessary for work to succeed. The second step is to characterize the variability of the functions from step 1. The third step is to assess how the variability of each function affects the variability of the system as a whole. The fourth step is to identify ways to manage the possible uncontrolled performance variability.

Identifying the functions includes a detailed breakdown of the functions or activities required for work to happen. This should be based on “work as done” instead of “work as imagined” or work as planned. In the case of risk assessment, it is impossible to know how work is done if it hasn’t happened yet, so it should be based on how work is likely done. The function should be described in terms of the 6 parameters displayed in Figure 2.1: inputs, preconditions, time, resources, controls and outputs. Inputs are items that are processed, transformed or needed to start the function. The output is the result of the function, which can be an entity or change of state. Preconditions are conditions that must exist before the function can be executed. Resources are consumed during the function to produce the output. Time is the temporal constraints on the function, with respect to the starting time, finishing time or duration. The control identifies ways that the function is monitored or controlled.

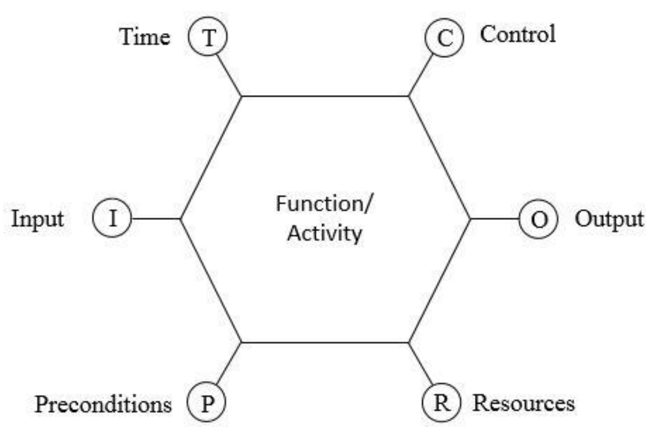


Figure 2.1: FRAM function diagram

The functions then may be coupled if the descriptions of the parameters are common for two or more functions. For example, if function A has an output that is an input or precondition for function B, then there would be coupling between function A and B. The coupling can be represented graphically by connections of one or more of the parameters from each function.

The variability then needs to be assessed for each function. The variability of the output of the function is what should be assessed, rather than the variability of the function itself. The variability of the output can be a result of the function variability (step 2), the working environment variability (step 2) or variability from coupled functions (step 3). The functions should first be characterized into one of three categories: technical functions, human functions or organizational functions. The variability can then be assessed by one of two methods: a simple method or a more elaborate method. The simple method only provides assessment of the variability in the function output in terms of time and precision. The elaborate method considers four categories for the output variability: 1) timing and duration; 2) force, distance and direction; 3) object; and 4) sequence. Then the variability due to function coupling should be assessed (Hollnagel, 2012).

If the analysis indicates uncontrolled performance variability - functional resonance - methods should be determined to manage the variability. Solutions should be sought to dampen the variability, or to control the performance variability if the outcome is expected to be beneficial. This can be done by adjusting the function parameters to produce a more consistent output. Due to the inherent variability in processes and their interactions, adjustments must be made to everyday work to maintain a functioning workplace. By understanding the system variability and identifying how to control it, safety can be achieved.

2.5. Case Study

A propane feed system was examined using FT and BN modelling from Khakzad et al. (2011). The probabilistic modeling will be referred to as it is seen in that work. The propane feed control system consists of an automatic control system that is the primary or desired control system. In the event that the automatic system is unavailable, or not functioning properly, a manual control system can be used to maintain the propane feed control. These models describe the components of the system and predict the probability of improper control of the propane feed system. In the FT analysis (Table 2.1 and Figure 2.2), the basic component failure probabilities are given and the system failure probability is computed by logical “and/or” operators for the faults. The BN (Figure 2.3) uses conditional probability tables to relate the individual component failure probabilities to overall system failure probability. Generalized system failure probabilities are then computed for a propane feed control system with automatic and manual control systems.

Table 2.1: System components of propane feed control system (Khakzad, Khan, & Amyotte, 2011)

Component	Symbol	Probability
Pressure transmitter failure	PT	0.1647
Pressure controller failure	PC	0.2818
No signal received by pressure controller	PC_signal	OR-gate
Pressure relay failure	PY	0.1538

No signal received by actuator	Act_signal	OR-gate
Automatic valve mechanical failure	A_valve	0.3403
Actuator mechanical failure	Actuator	0.2015
Automatic valve improper control	A_valve_ctrl	OR-gate
Human failure in operating manual valve	Hum_err	0.2696
Manual valve mechanical failure	M_valve	0.1393
Manual valve improper control	M_valve_ctrl	OR-gate
Feed system improper control	Feed_ctrl	AND-gate

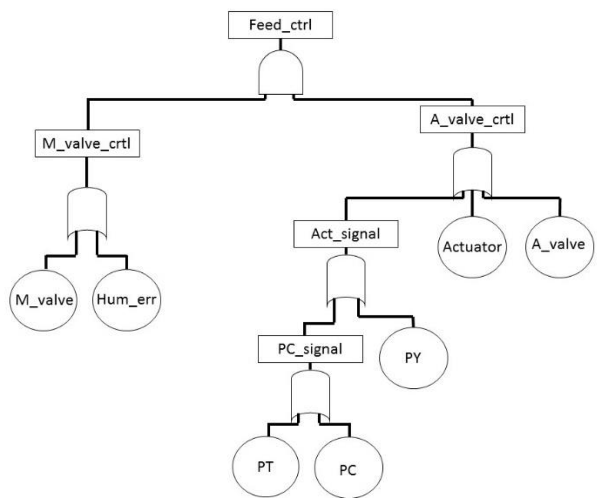


Figure 2.2: Fault tree of propane feed control system (Khakzad et al., 2011)

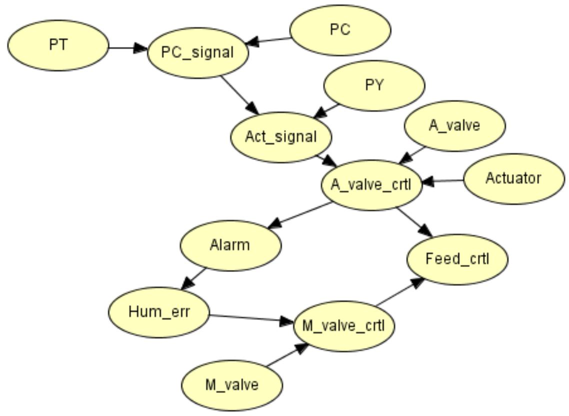


Figure 2.3: Bayesian network of propane feed control system with an alarm added (Khakzad et al., 2011)

In generalized safety models, the context of the application is usually neglected or not considered to the extent that it should be. If we take the failure of the pressure controller to be 0.2818, as indicated in Table 2.1, is this true for all propane feed control systems? If the pressure controllers are purchased from different manufacturers, or a higher quality product is chosen, would that affect the component reliability? If the pressure controller is misused, or is poorly maintained, would that affect the component reliability? The probability of 0.2818 is a generalized value which is estimated from the failure data of many pressure controllers irrespective of the context. Some of the pressure controllers in this data set might not have been used in propane feed systems, but completely different systems.

Context becomes even more relevant when considering human behavior and decision making. The propane feed control system is designed such that if there is a failure of a technical component in the automatic feed system, the manual feed system will be engaged by a worker to maintain the system control. All the human elements in this system are described by a single node called "human error." What is the context of this human error?

Is it just that humans make an error 26.96 % of the time (Table 2.1)? It is not completely clear what is meant by human error in this context and it provides little guidance to improve the human reliability.

Another method that can be used to examine this system is the Functional Resonance Analysis Method (FRAM). By doing this, an additional and more informed understanding of the system can be gained. Rather than describing the system by its components, FRAM describes the system in terms of the functions that the components carry out. The system is broken down into the functions that are carried out by technology, humans and organizations. The technical components of the propane feed system can carry out all the functions necessary to operate the control system. The manual control system monitors the automatic control system and relies on an operator to adjust the propane flow in the event that the automatic system cannot control it. See Figure 2.4 for FRAM representation of the propane feed control system and Appendix B for the description of the functions and coupling.

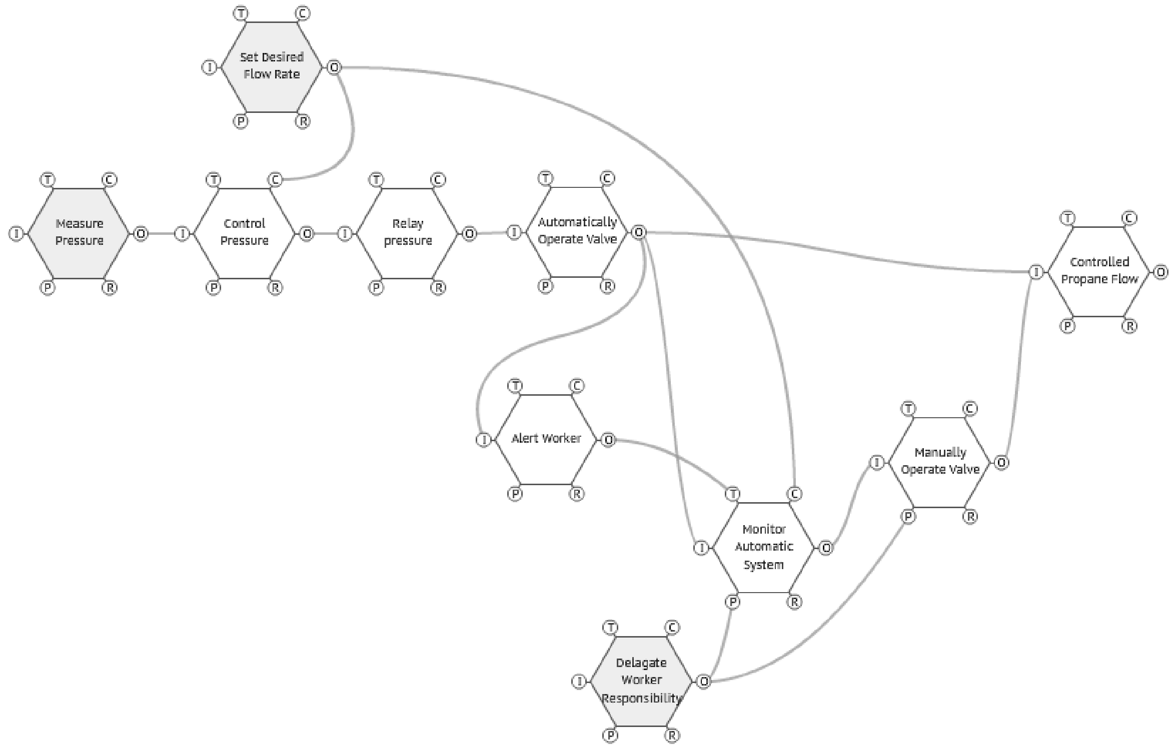


Figure 2.4: FRAM model of propane feed control system

The next step in FRAM modelling is to assess the function variability. The variability of the function outputs should be examined with respect to time and precision. The output may be produced on time, too early, too late, or not at all with respect to time. The output may also be precise, acceptable or imprecise with respect to precision. A change in the output variability could produce variability in the overall system performance, but not necessarily system failure. When considering the potential variability, it is possible that the output could potentially be either of the states listed with respect to time and precision. The function variability requires context to assess fully. Examining a case or set of cases will provide insight to the adjustments that need to be made regularly within a system due to variability in the outputs. Even though this generalized propane feed control model lacks specific context, the potential functional resonance (significant performance variability) can be assessed at some level of detail.

To illustrate, we consider that the automatic control system is composed of a series of technical components, and at some point at least one of the essential components will fail. In order to maintain functionality of the system, the manual control system must be engaged to control the flow. This requires that the operator is aware of the automatic system failure in time to make corrective action. This makes monitoring the automatic control system crucial to maintaining the propane flow control. One potential instance of improper propane control is if the pressure sensor fails in the automatic system this could also affect the ability to monitor the system. If the pressure sensor is the signal that alerts the worker that the automatic system has malfunctioned, failure of that component could disable both the automatic and manual systems. It is not exactly stated which components in the automatic system are monitored to indicate the automatic system performance to the worker. However, it can significantly affect the system reliability and system performance. A solution to this is to add another pressure sensor to indicate the system pressure to the alarm and notify the worker and also provide direct feedback to the worker for monitoring purposes (Figure 2.5). With this modification, the failure of a single component does not affect both the automatic and manual feed control systems. Another important question that is evident when assessing this system is: where is the sensor located within the system? Is it in the best place to correctly signal over-pressure situations to the alarm? Or is more monitoring required? Describing the work in terms of the functions and the system variability helps to identify situations where the component may not have failed but it failed to complete its task due to poor system design.

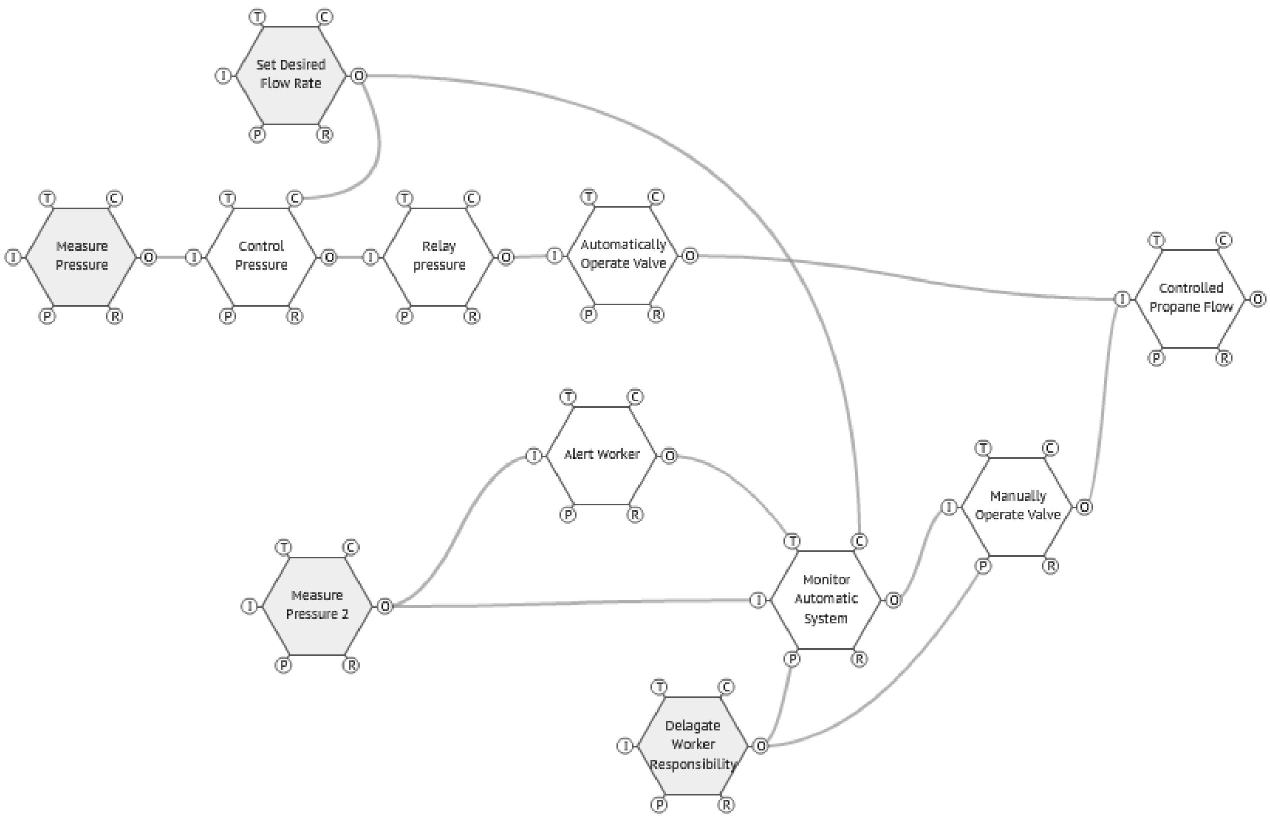


Figure 2.5: FRAM model of propane feed control system with design adjustment

We can transfer the modified system back to the fault tree representation, as shown in Figure 2.6. The human error component which was previously a primary event, has been converted to an intermediate event. This requires that probability of human error is now computed by the logical operators connecting the primary events of alarm failure, PA, and the additional pressure sensor, PT2. This representation of the system yields a probability of improper feed control of 0.1418. This assumes that the probability of alarm failure is

0.2614, and the probability of failure of PT2 is equal to PT (Khakzad et al., 2011). There is also an assumption that a human error will occur as a result of the failure of both the alarm system and the secondary pressure sensor. It could be that a human error will occur with the failure of the alarm system or the secondary pressure sensor, or a human error may occur that is not related to either of the two events. These scenarios would require additional fault trees to be developed compute the other possible probabilities of improper propane feed control, making this modelling technique quite cumbersome.

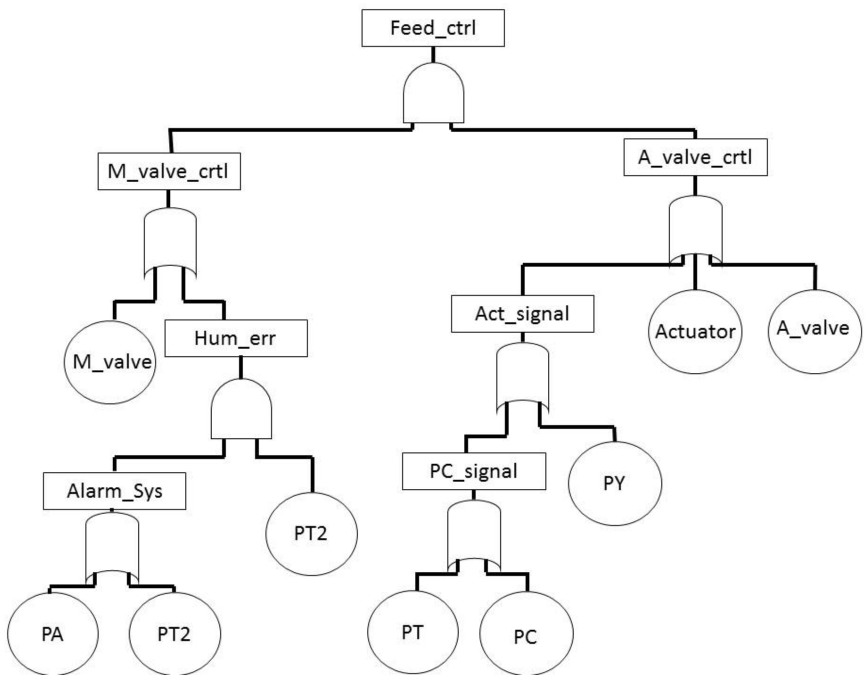


Figure 2.6: Updated fault tree with alarm and extra sensor

Now consider this system as represented by a Bayesian Network (Figure 2.7). The Bayesian Network is a more robust modelling technique than the Fault Tree. It can accommodate more direct and complex dependencies between factors. Using the conditional probability tables, more complex relationships can be modelled than with logical operators. The Bayesian Network can also incorporate higher order factors, where as a fault tree can only consider binary. These benefits of the Bayesian network are seen when modeling the alarm and the human error factors. The Alarm has 3 states: No sound, Wrong sound, and Right sound. The alarm and human error are also conditioned such that relationships do not strictly adhere to the logical operations seen in the fault tree (Khakzad et al., 2011). This analysis in Figure 2.7 yielded a probability of improper feed control of 0.1042.

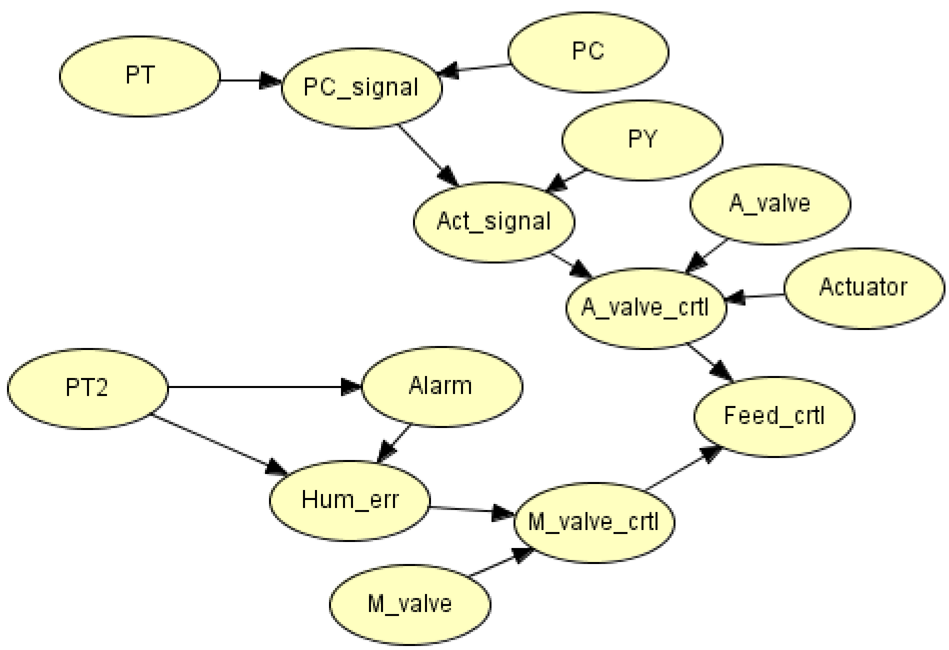


Figure 2.7: Updated Bayesian Network with extra sensor

There are other ways the system could fail to function even with the system as depicted in Figure 2.5: Both pressure sensors could fail, both valves could fail, the worker may not be present at the time of automatic system failure, or the worker may be distracted by other tasks which affects his ability to monitor the system. Depending on the consequences and context of the situation, it may be appropriate to add a pressure rupture disk, or a safety system that requires a worker to be present for the system to operate at all. In this analysis, organizational factors were not considered as it would depend on the context of which regulations apply and which companies are the acting operators. The organizational factors can be considered in FRAM by including the functions that those organizational entities carry out.

2.6. Discussion

Three modern techniques were used to assess the safety of a propane feed control system. One main difference between the techniques is the treatment of the human factor, and organizational factor, although the focus here has been on the human factor. The fault tree uses discrete logical operators and assumes that all factors are binary. There are methods to adopt fuzzy logic to fault trees, but this requires that distributions are known to model the factor dependencies. This is often unknown for the human element and given that work is often under-specified, there are times it cannot be known. The Bayesian network approach is an improvement on the fault tree approach. It can better model complex factor dependencies using conditional probability tables, however it encounters similar issues as the fault tree approach using fuzzy logic given that all the conditions may not be known. The Bayesian network allows for factors that are higher order than binary, as seen with the alarm. The FRAM approach provides a framework that allows the human interaction in the system to be more easily understood, by describing the work. The human element is essential to successful operations and needs to be considered as more than a component that can only succeed or fail. FRAM can better describe complex human-technological interactions within a system and then more informed safety solutions can be identified.

It should be noted that the FRAM analysis was only partially completed in this case study. Step 1, the functional description of the system was completed and only one instance of variability was considered, a pressure sensor failure. It is not practical to hypothesize about the range of normal variability that could be seen during the operation of a propane feed control system. In practice, information about variability should come from the workers who perform the work to represent the actual variability and not the imagined variability. In this case, the propane feed system is a hypothetical system, referring to any propane feed system that contains the same components. Therefore, the analysis was truncated after this one instance of variability as there were no workers to verify imagined variability claims. This level of analysis was also sufficient to illustrate the building of the FRAM system and the perspective that is gained from using FRAM.

In section 2.5 a modification was made to the original safety analysis (Khakzad et al., 2011) based on the insights identified using the FRAM analysis. An improvement from 0.2720 to 0.1418 was made in terms of the estimated probability of improper propane feed control as modeled using the fault tree approach. A slight improvement was observed when the modified system was analyzed using the Bayesian network approach, from 0.1146 to 0.1042. However, there was no data to update the conditional probability tables for this updated system, so the results were unlikely to change significantly. When new system conditions are identified or proposed, the previous data may become irrelevant if it was collected under different conditions, which is a drawback of probabilistic techniques.

FRAM is a technique that can be used to understand new systems in terms of why they may fail and also why they should work. Given that industrial workplaces are constantly evolving, it is important to assess new (present) systems without invoking biases from older systems. This adaptable approach provides balanced consideration of the factors present in socio-technical systems and has the ability to assess new and evolving conditions in industrial safety. By considering this alternative perspective in FRAM additional information can be revealed which can help inform safety assessments. This bottom-up approach can complement the top-down approaches of the FT and BN if they are needed.

2.6.1. Human Factor

When studying industrial accidents, it becomes evident that humans have played a major role in past accidents. Many quotes can be found in the literature referencing the high percentage of accidents that are caused or contributed to by human error, regardless of industry.

"…Somewhere between 70-80% of all aviation accident are attributed, at least in part, to human error…" (Shappell and Wiegmann, 2004)

"…About 80 percent of all events are attributed to human error. In some industries, this number is closer to 90 percent…" (U.S. Department of Energy (DOE), 2009)

"…About 75-96% of marine casualties are caused, at least in part, by some form of human error…" (Rothblum, 2000)

Given the high percentage of accidents that are being attributed to human error, it is important that careful consideration is given to how the human element is incorporated into modern safety assessments. In socio-technical systems, humans do not function in the same way that a technical component does. Humans are necessary in industrial workplaces to adapt to unexpected events and maintain functionality. The expectation is that humans act on the many conditions that may be present in the workplace, some of which do not have prescribed solutions. Then success or failure may be assigned to human actions by the determination of how favorable or unfavorable an outcome is. FRAM uses a structured framework to understand how human actions effect the success and failures of industrial operations. To improve the understanding of the human factor more, information about the work and variability should be collected from the operators to understand how work actually happens. However, this is not done in this analysis.

2.6.2. Emergence

Given the level of detail that has been presented in this comparison the FRAM analysis may appear to be less complete than the BN and FT analysis. The FT and BN analysis produces quantifiable results that estimate the chance of system failure occurring. This quantification gives closure to the analysis, but does it provide enough insight to make suggestions to adequately improve the safety? The probabilities are difficult to verify in complex socio-technical systems. The structure of the FT and BN models are developed from a prior understanding of the operations. This structure then allows the probabilities to be estimated by searching for the data that is deemed important by your prior understanding. Then probabilities reflect your prior belief of the influence that certain system components have on causing accidents. Of course the BN approach does give the ability to update the probabilities with new data but data will only be collected for the components that are believed to be important. Given the evolving nature of industrial workplaces complete understanding will be difficult to achieve, but additional information can be obtained, which will strengthen the understanding.

In the FRAM approach, the insight that is provided in Section 3 is that accidents do not result directly from the existence of certain components in a system. In fact, the presence of these components make the system likely to succeed most often. The understanding of the accident is contained within the interactions of the system components. In FRAM, the interaction is examined through the variability of the system outputs from the functions and the coupling with downstream functions. At the level of detail of these analyses (constant for FT, BN and FRAM), the variability is not sufficiently defined. To understand the variability of the system more details are required. As the level of detail is increased and understood the actual causes of the accidents will start to emerge. This property of emergent accident theories can improve our understanding as we are forced to seek more details to achieve higher understanding of events

2.6.3. Functional Resonance

In section 2.4.1 functional resonance is likened to stochastic resonance. In stochastic resonance, many (weak) signals of random noise can be combined to form a system of noisy signals. When the signals combine, occasionally there will be “resonant spikes” in the overall system signal that appear much larger in magnitude than the weaker noisy signals that have been inputted. This resonance is a function of random frequency and weak (yet variable) amplitude noise. For functional resonance, the signals are not random. They are the variable outputs of the system functions, also in some cases the variability may be hard to define continuously (unlike stochastic noise). The functional output with no variably is to produce the output exactly in terms of precision and the time it is required to be produced. Such exact outputs are rarely achievable in practice and it would be poor design to require such exactness. The functional output can also be some lower precision, roughly timed variation of the idealized (imagined) output. The output can vary to the point where there is no output produced – a functional failure. A functional failure alone does not necessarily indicate resonance, as most systems are resilient enough to accommodate localized failure with minimal effect on the overall system performance. I.e. a failure of a single component in the automatic propane feed control system will likely not affect the performance of the entire system because the manual system will be activated and propane flow will be regulated manually achieving good performance for the system. However, resonance can occur when the variability of a single function combines with other functions to produce a significantly different effect on the overall system. I.e. when we consider a potential pressure sensor failure, it has the potential to effect the performance of the alarm system (if that pressure sensor is also used in the alarm system), which would also effect the chance that the worker notices the improper pressure situation, increasing the chance of improper propane control in both the automatic and manual systems – functional resonance. In the manuscript, a second pressure sensor was added to the alarm system to minimize the chance of this resonance scenario.

2.6.4. Failure vs. Success

In the FT and BN approaches a premium is placed on examining details of the accidents (failures) which does make sense, but the successes are often ignored and considered less valuable. In fact, there is a lot of information that can be learned from the successes, some of which may be critical to accident prevention. Successes are examined in FRAM by understanding the functions that are necessary for work to succeed. The quantification of the FT and BN should be representative of both successes and failures. Given that the probability of failure is the ratio of failures to the sum of successes and failures, it should require that the successes be considered as well. To better understand industrial safety, the details of the successes should be examined and not just the number of successes. If we are to study safety we should examine the cases where safety is actually present (successes) and by studying the accidents we are studying the absence of safety (Hollnagel, 2014b). Actually, both successes and failures should be examined extensively to better understand safety and accidents and improve industrial safety assessments.

Approaching safety by understanding the successes and prescribing strategies to have future success may be more effective (or at least more comprehensive) than prescribing strategies to not fail. If we consider that operational success is defined by achieving one or more goals that may be prescribed by the operation. In practice, the goals are not always achieved by the idealized definitions but by achieving them within some acceptable tolerance. Once the acceptable limits are exceeded, the operation will be labeled a failure. By this definition, prescribing strategies to succeed becomes a bounded problem whereas prescribing strategies to not fail is unbounded. This is a technique that has been proposed by others in the past as a proactive risk management strategy (Rasmussen and Svedung, 2000). Such a strategy is well suited for FRAM as well. Figure 2.8 displays this definition for operational success and failure. In FRAM each function requires some objective to be completed – and output to be produced which has some idealized expectation of the output.

Each function can represent an axis with a variable scale. When the function produces the exact imagined output, that point would be located at the origin. Once we notice imprecise variations of the output occurring the point on that axis starts to move away from the origin based on the deviation from the expected value. By doing this for each function in the system we can define the state of variability at a given time. Then it is important to understand the amount and type of variability that the system can accommodate (resilience). This defines the acceptable limits of the operation. If the state of variability is completely inside of the acceptable operational limits, conditions would be met to define success. Once the variability starts to exceed the acceptable limits, conditions would define failure. Additionally, it may be difficult to exactly define what the limits of the operation are, so there will be a so called grey area or blunt boundary.

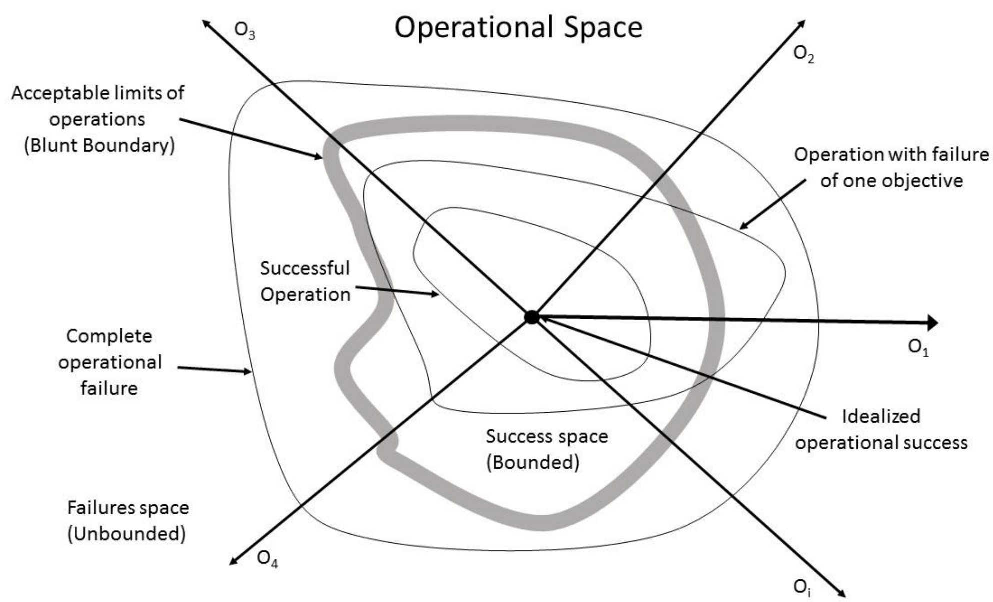


Figure 2.8: Defining operational success vs. operational failure

Learning from the successes also improves the rate at which we can learn. The rate at which successes occur is much higher than the rate at which failures occur. And if we consider both we are constantly learning. Practically, if we are to examine the failures extensively, we are not only limited to the rate at which accidents occur we are limited to the rate at which accidents are reported. Consider the ratio of accident cases categorized by decreasing severity respectively, accident, incident, and near miss, as in Heinrich's triangle (Heinrich, 1931). While the proportions of these accident cases may or may not resemble the triangle distribution proposed by Heinrich, it can be used to illustrate another feature of FRAM. We may consider that accidents and incidents are typically reported because the severity of the outcome is noticeable. The number of near misses may not be accurately reported because the near miss does not produce an outcome that is noticeably different from a success (Figure 2.9). Some proportion of these near misses will not be noticed in a methodology that focuses on unfavorable outcomes. In Figure 2.9 the shape and relative sizes of these events are chosen arbitrarily, and is just for illustrative purposes. The near misses that would otherwise be unnoticed can be found in the FRAM approach through variability for a successful outcome. Variations within the system which required adjustments to be made to maintain the system functionality represent the normal system variability including many near misses.

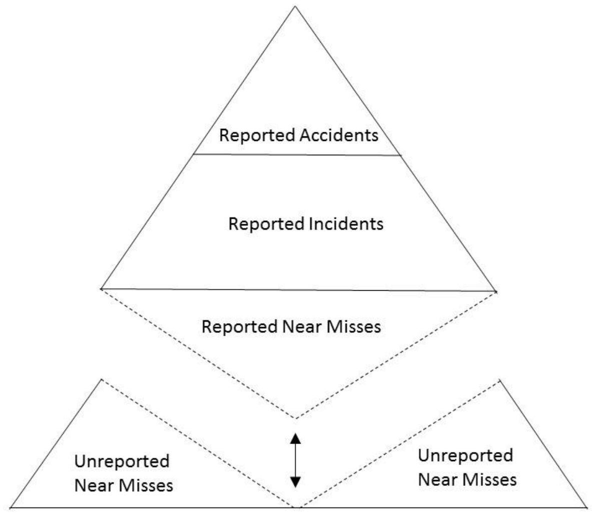


Figure 2.9: Accident triangle visualization of unreported near misses

2.6.5. Method Comparison

While using this case study as a comparison of three modern assessment methods it may be useful to compare the methods directly as seen in Table 2.2. It may not stand out that there is one method better than the other. Each method can be useful and can be used as a tool to help inform safety assessors. They are different methods that help us understand different things and the most appropriate approach would be to use the information uncovered by each synergistically.

Table 2.2: Comparison of the methods

	Amount of information required	Type of information required	Accident explanation	Focus of investigation	Guided system description	Quantifiable

Fault Tree	lowest	components, logical relationships and individual failure data	Causal	Failure	No	Yes
Bayesian Network	more	components and CPT's	Causal	Failure	No	Yes
FRAM	most	Functions, functional interactions and variability	Emergent	Failure and success	Yes	No

The FRAM can at times appear less complete, as it did in this case study but that that is because it requires more information to fulfill the analysis. This is not necessarily a down fall of the method because by trying to understand the extra information, in terms of functionality and understanding the successes, we asked, how is the alarm system being actuated? This was shown in the case study to be an important element to consider. The use of emergent accident explanations can discourage the acceptance of weaker explanations for accidents. While the BN and FT look to explain events using causal chains, what they often produce are chains of probably cause. By seeking stronger explanations and making them emerge from better understanding, important information can be uncovered to strengthen causal chains. Also, Quantification can be good as long as it is being informed appropriately. But, misinformed quantification can be quite dangerous as it implies that an analysis has been conducted and all the necessary information has been reduced to a single (or interval) quantifiable result. This was seen in the Challenger space shuttle disaster. The management team decided to believe that the chances of rocket booster failure when launching at the cold temperature that morning was roughly 1 in 1000000 (misinformed quantification). When it was revealed later that engineers told management that the chances were more likely to be 1 in 1000 (more informed). And the result of this accident was partially (if not directly) influenced by misinformed quantification (Feynman, 1999). Also, in terms of the guidance provided to understand the system FRAM helps the investigation by telling the assessor what to look for. The FT and BN are merely vehicles to support quantification and require all qualitative understanding of the system to be tackled with little guidance.

2.7. Conclusions

The continual evolution of socio-technical systems requires safety assessments to evolve to stay relevant. From a case study of a propane feed control system using modern accident analysis methods, it can be seen that adaptive methods such as FRAM can be adopted to highlight system vulnerabilities that may be present. This method is not limited to learning from past failure; there can also be learning from successful operations. In many industries, operational limits are being pushed as technologies evolve. This invokes new conditions that may have high uncertainties in the system. Given that there may be little known about these new conditions, adaptive approaches may be used to suggest safety solutions.

The comparison of the three techniques highlights some of their strengths and weaknesses. FT and BN analyses of a propane feed control system from Khakzad et al. (2011) was used as a reference case. The FRAM method was used to identify some potential vulnerabilities in the propane feed control system, then these new systems were modelled using the fault tree and Bayesian network approaches. It was also identified that context is important when considering system safety. Context is gained through the incorporation of the details that are necessary to provide understanding of the operations in FRAM. There could be propane feed control systems that are both low risk and high risk that contain the same components. How the components are used, connected, and managed can influence the safety assessment and the operations. Adaptive approaches make this more evident and allow the context to be considered in more detail. This can become even more important when considering larger systems, such as an entire propane plant or a sector of the transportation industry.

FRAM provides a framework that makes complex human-technical relationships easier to identify. Identifying these complex relationships is essential to understanding how accident scenarios emerge. Proper monitoring strategies and resilient design solutions may then be offered to improve system safety. FRAM provides an alternative perspective to safe operations that can improve understanding which is the basis of any safety assessment. To perform the most comprehensive safety assessments, knowledge of both the operational successes and failures are needed.

While there is value that can be gained from using any of the methods discussed in this paper. It is more important that the assessors be cognizant of the utility of each method. Each method may help uncover various pieces of the puzzle that is to understand industrial safety. The challenge we are faced with is to keep up with the evolving nature and increasing complexity of modern industries. FT and BN are currently staples in the risk community but will likely have trouble keeping pace with industries and staying relevant. It may also be desirable to adopt FRAM in the toolbox of safety assessors. Synergistically, FRAM can be used to help keep up, by learning from successes, helping to monitor operations (including unreported near misses), and seeking stronger explanations for accidents. This can improve the overall understanding of the system and in turn strengthen any quantifiable analysis that is desired.

2.8. Acknowledgments

The financial support of the Lloyd's Register Foundation is acknowledged with gratitude. Lloyd's Register Foundation helps to protect life and property by supporting engineering-related education, public engagement and the application of research.

2.9. References

Borys, D., Else, D., Leggett, S., 2009. The fifth age of safety: the adaptive age. J. Health Saf. Res. Pract. 1.

Cooper, S.E., Ramey-Smith, A.M., Wreathall, J., Parry, G.W., Bley, D.C., Luckas, W.J., Taylor, J.H., Barriere, M.T., 1996. A Technique for Human Error Analysis (ATHEANA) (No. NUREG/CR-6350). Brookhaven National Laboratory, Upton, NY.

Feynman, R.P., 1999. The Pleasure of Finding Things Out: The Best Short Works of Richard P. Feynman. Basic Books, New York.

Glendon, A.I., Clarke, S., McKenna, E., 2006. Human Safety and Risk Management, Second Edition. ed. CRC Press, Boca Raton, FL.

Hale, A.R., Hovden, J., 1998. Management and culture: the third age of safety. A review of approaches to organizational aspects of safety, health and environment, in: Occupational Injury. Taylor and Francis, London.

Heinrich, H.W., 1931. Industrial accident prevention: a scientific approach. McGraw-Hill, New York.

Hollnagel, E., 2014a. Safety-I and Safety-II: The Past and Future of Safety Management, 1st ed. Ashgate Publishing Ltd., Farnham, Surrey, UK England ; Burlington, VT, USA.

Hollnagel, E., 2014b. Is safety a subject for science? Saf. Sci., The Foundations of Safety Science 67, 21–24. doi:10.1016/j.ssci.2013.07.025

Hollnagel, E., 2012. FRAM: The Functional Resonance Analysis Method. Ashgate Publishing Ltd.

Hollnagel, E., 1998. Cognitive Reliability and Error Analysis Method, 1st ed. Elsevier Science Ltd., Oxford.

Hollnagel, E., Woods, D.D., Leveson, N., 2006. Resilience Engineering: Concepts and Precepts. Ashgate Publishing Ltd., Hampshire, UK.

Human Performance Improvement Handbook - Volume 1: Concepts and Principles (No. DOE-HDBK-1028-2009), 2009. . U.S. Department of Energy, Washington, D.C.

Khakzad, N., Khan, F., Amyotte, P., 2011. Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches. Reliab. Eng. Syst. Saf. 96, 925–932. doi:10.1016/j.ress.2011.03.012

Khan, F.I., Amyotte, P.R., DiMattia, D.G., 2006. HEPI: A new tool for human error probability calculation for offshore operation. Saf. Sci. 44, 313–334. doi:10.1016/j.ssci.2005.10.008

Louisell, D., Anderson, K., 1953. The Safety Appliance Act and the FELA: A Plea for Clarification. Law Contemp. Probl. 18, 281–295.

Meshkati, N., 1991. Human factors in large-scale technological systems' accidents: Three Mile Island, Bhopal, Chernobyl. Organ. Environ. 5, 133–154. doi:10.1177/108602669100500203

Rasmussen, J., Svedung, I., 2000. Proactive Risk Management in a Dynamic Society. Swedish Rescue Services Agency, Place of publication not identified.

Rothblum, A.M., 2000. Human Error and Marine Safety. Presented at the National Safety Council Congress and Expo, Orlando, USA.

Shappell, S., Wiegmann, D., 2004. HFACS Analysis of Military and Civilian Aviation Accidents: A North American Comparison. Presented at the ISASI Seminar, Gold Coast, Austrailia.

Speegle, M., 2012. Safety, Health, and Environmental Concepts for the Process Industry. Cengage Learning.

Swain, A.D., 1963. A Method for Performing a Human Factors Reliability Analysis (No. Monograph SCR-686). Sandia National Laboratories, Albuquerque.

Swain, A.D., Guttman, H.E., 1983. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications (THERP) Final Report (No. NUREG/CR-1278). US Nuclear Regulatory Commission, Washington, DC.

Underwood, P., Waterson, P., 2013. Systemic accident analysis: Examining the gap between research and practice. Accid. Anal. Prev. 55, 154–164. doi:10.1016/j.aap.2013.02.041

US Nuclear Regulatory Commission, 2013. Three Mile Island Accident Backgrounder (Fact Sheet). US Nuclear Regulatory Commission.

3. USING THE FRAM TO UNDERSTAND ARCTIC SHIP NAVIGATION: ASSESSING WORK PROCESSES DURING THE EXXON VALDEZ GROUNDING

3.1. Co-authorship statement

A version of this manuscript has been published in the International Journal on Marine Navigation and Safety of Sea Transportation (TRANSNAV), written by authors, Doug Smith, Brian Veitch, Faisal Khan, and Rocky Taylor. Author Doug Smith led the writing of this manuscript, including development of the methodology, performing interviews with ship navigators, building the FRAM model for ship navigation, capturing the variability for the FRAM model, and producing the model case study using the Exxon Valdez grounding. All authors revised, edited, discussed this work and made recommendations for improvements to its presentation.

3.2. Abstract

Arctic shipping involves a complex combination of inter-related factors that need to be managed correctly for operations to succeed. In this paper, the Functional Resonance Analysis Method (FRAM) is used to assess the combination of human, technical, and organizational factors that constitute a shipping operation. A methodology is presented on how to apply the FRAM to a domain, with a focus on ship navigation. The method draws on ship navigators to inform the building of the model and to learn about practical variations that must be managed to effectively navigate a ship. The Exxon Valdez case is used to

illustrate the model's utility and provide some context to the information gathered by this investigation. The functional signature of the work processes of the Exxon Valdez on the night of the grounding is presented. This shows the functional dynamics of that particular ship navigation case, and serves to illustrate how the FRAM approach can provide another perspective on the safety of complex operations.

3.3. Introduction

The Arctic may become integral part of the shipping industry on a global scale if current climate trends continue. If that does happen it will involve a transitional period, where many lessons will be learned as the boundaries of normal shipping operations are broadened. Experienced shipping in the Arctic is limited, information is scarce, and not widely shared. In order to become prepared for such an increase in shipping traffic in the Arctic (and Antarctic), information we do have should be examined as thoroughly as possible. This may help us better understand the conditions and how to operate in them.

The present work uses the Functional Resonance Analysis Method (FRAM) to build an understanding of Arctic ship navigation and uses the Exxon Valdez grounding as a case to examine the model's utility. This work is intended to initiate discussion across the maritime domain about FRAM and understanding Arctic operations. We can use the FRAM to help understand different elements of ship navigation, including the so called "soft factors," which are difficult to assess with traditional techniques. This will become even more important when considering Arctic shipping because the information is both vague and scarce (Arctic Council, 2009). The FRAM provides a structured framework to consider anecdotal experience from successful shipping operations, which can help formalize lessons learned and share them across the domain. By consolidating information across the domain it will improve our understanding of shipping safety. By improving our understanding this way, we can then improve ship operations (the way they function) and safety in the maritime domain.

3.4. Background

A shipping operation is a socio-technical system that requires many combinations of social and technical factors to be managed to succeed. There has been a movement towards adaptive approaches to safety to help manage such systems (Borys et al., 2009). This approach relies on not only modeling the elements in the system, but the relationships in the system, eg. how elements interact together (Vicente, 2004). Because of this shift in thinking, other techniques are being adopted from resilience engineering to help manage complex systems as well (Ayyub, 2014, 2015; Hollnagel et al., 2006).

Additionally, there is acceptance that many of the conditions that operations are being subjected to are so dynamic that it is very difficult to prescribe a single safety protocol to manage them. The Society of Risk Analyst's recent review states that in these cases it is better to have a dynamic set of solutions to adapt to these dynamic conditions (Aven et al., 2015). Safety is then approached by understanding how to best monitor areas of the system and how to control them: in other words, by designing systems that adapt (or maintain control) when subjected to dynamic conditions.

There are a number of methods that are founded on adaptive safety methodologies: the Functional Resonance Analysis Method (FRAM), Systems-Technical Accident Model and

Processes (STAMP), and Human-Tech approach (Hollnagel, 2012; Leveson, 2004; Vicente, 2004, respectively). Each method has the potential to improve safety by incorporating systems thinking into the approach. In this paper the FRAM is used to perform an investigation of ship navigation in the Arctic. The FRAM was chosen for two reasons: 1) it focuses on functionality, and 2) it promotes communication between assessors and workers. To understand functionality, you must understand the conditions that can be operated in, and the conditions that cause problems. This means that accident events should not be isolated from the typical operational outcomes to develop understanding of accident mechanisms. By isolating the accidents, biases may enter the interpretations of events. Safety solutions should show consideration of both the event(s) one would like to prevent and promotion of the event(s) one would like to achieve. When understanding functionality, it is best to obtain an understanding from the operational perspective. This concept promotes understanding the work as it is done, rather than as it is imagined by assessors. This can help reduce the communication gap that exists between assessors and operators, thereby, promoting safety solutions that are grounded in reality.

3.4.1. FRAM

The FRAM is built on identifying functional resonance. Functional resonance is an analogy to stochastic resonance, where multiple signals of low amplitude noise are inputted to a system and, if resonance occurs, the overall system signal can have a much greater amplitude. In functional resonance, the output of the system functions are variable and slight variations between the many functions in a system have the potential to combine in such a way that resonance occurs. The resonance will be some variation of the overall system performance that goes beyond what is typical or expected, regardless of whether the outcome is viewed as good or bad. By modeling the system functions and variability in sufficient detail, safety solutions will emerge that focus on monitoring and controlling the system.

The FRAM is based on four underlying principles (Hollnagel, 2012):

- Failures and successes are equivalent in the way that they happen for the same reason. Alternatively, it can be said that things go wrong for the same reasons that they go right.
- Daily performance of socio-technical systems, including humans individually and collectively, is always adjusted to match the system conditions.
- Many of the outcomes of the system that we notice, and also the ones we don't notice, are emergent rather than resultant.
- Relations and dependencies must be described as they develop in a particular situation and not as cause-effect links. This is done through functional resonance.

The first step of the FRAM is to describe the functions of the system and the aspects of the functions that occur when work happens. Each function can have 6 aspects that should be considered, as seen in Figure 3.1.

Output: Each function should have an output(s). If work is being done there should be something produced by the work. The outputs are then passed throughout the system and have the ability to affect other work in the system in 5 possible ways.

1) Input: The input starts the functions. If the input is an output that arrives late from another function, it will affect the functionality of the downstream function.
2) Preconditions: Preconditions must be available prior to the function starting, but they do not initiate the function. They can lay dormant in the system until the function begins.
3) Resources: These are things that are processed during the function. To limit the resources that are considered, focus should be placed on resources that are consumed and subsequently need to be resupplied by another function in the system. Resources such as computers, which are not consumed, should not considered here. They would be considered as execution conditions, which can be assessed when understanding the function itself.
4) Time: Other functional outputs have the potential to affect the available time to carry out a function.
5) Control: Other functions may interact with downstream functions in a way that acts as a control.

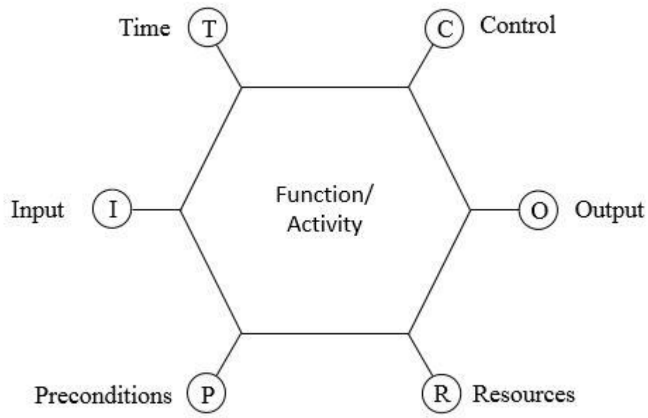


Figure 3.1: FRAM function diagram (Hollnagel, 2012)

After the system functions and aspects are described at some level of detail. The variability should be considered. Step 2 considers the internal variability of the function and the variety of ways an output can be produced under dynamic conditions. Step 3 assesses the coupled system variability, which is the way the variations from upstream functions can affect the downstream functions, and in turn the entire system performance. The final step is to identify appropriate ways to monitor the system and control the variability in it. In practice, it is very difficult to obtain all the necessary information at once, so this process may need to be repeated as new information is obtained.

3.5. Methodology

In order to build a FRAM model for Arctic ship navigation the following methodology was used. First, the scope was defined. Then the system functions and connections were imagined by the assessor(s). The conceptualized model was then checked with operators to verify that the model reflects the way the work is actually done. At this point, the model represented the potential functional paths that could be taken for the system to produce some outcome. Then the variability of the functional outcomes can be understood. It is best to learn about the variability of the functions by either monitoring the functional output directly or communicating with the workers who carry out each function. Once the functional model was built and some variability documented, the model was applied to cases. By examining cases through the lens of the FRAM, different findings may emerge that pertain to functional execution and system variability. These findings can then be used to either update the model, or manage the operation. This methodology is mapped out in Figure 3.2.

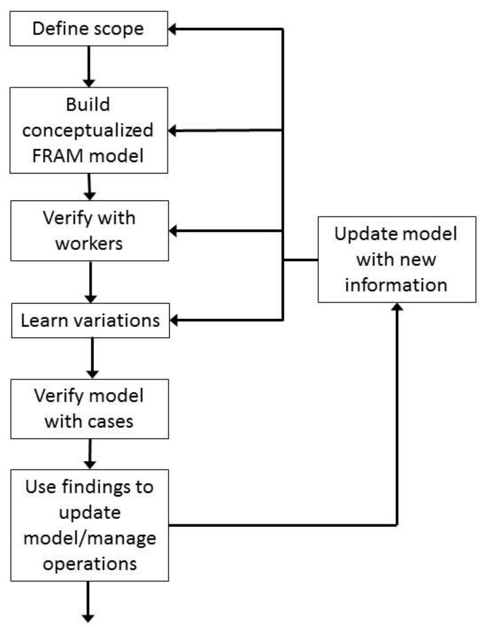


Figure 3.2: Methodology for building FRAM model

3.5.1. Defining the scope

The first step is to define the scope of the assessment. This assessment focuses on (Arctic) ship navigation. From a systemic perspective, there are many functions that influence the performance of a shipping operation and trying to model all of them at once could be overwhelming. As there is so much information to learn about the work that is carried out in a shipping operation, the initial assessment focuses on navigating the vessel. This is the most basic objective for a ship and all other work is complementary to it. This allows the initial understanding to reflect the most immediate functions required for navigation, and then the scope can be gradually broadened in the future. Also, the focus will be on transit shipping; stationary offshore installations are out of scope.

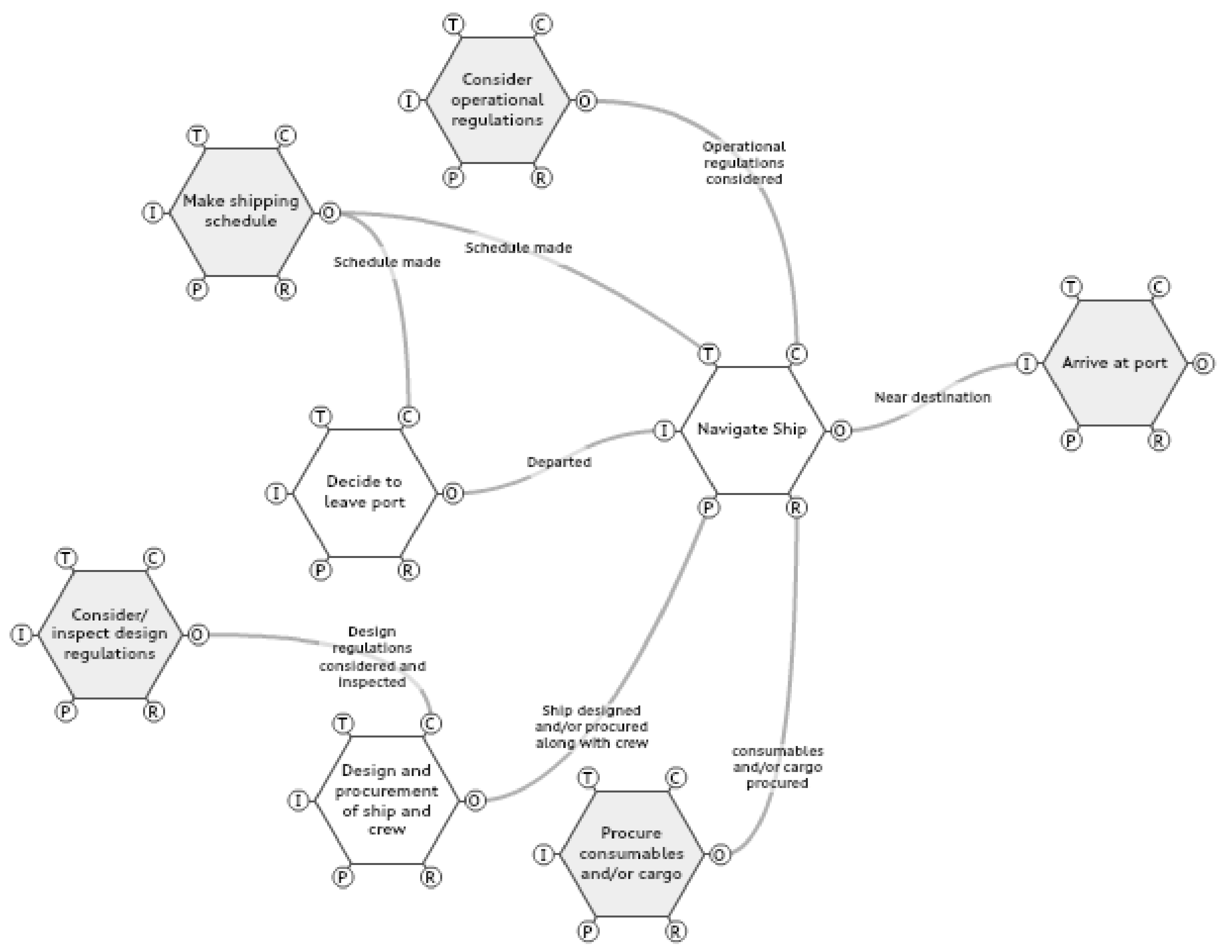


Figure 3.3: General ship navigation FRAM model (scope)

First, build a FRAM model to help define the scope (Figure 3.3). We define a function, "Navigate ship," which describes the function that is carried out to physically move the ship from port to port. Then we can define the aspects of the "Navigate ship" function. The output can be that the ship is now near the destination, and other functions involved in, "Arrive at port," can begin bringing the ship to the destination. The input is the function "Decide to leave port." While this decision to leave is influenced by the shipping schedule, the ship does not necessarily leave exactly when scheduled. Many factors could affect the time at which the ship actually leaves port, but this decision is controlled by the schedule. The time that this decision will be made will be roughly around the scheduled time, but could be ahead or behind schedule, due to inspections, cargo or consumable loading, etc. The shipping schedule can also influence the ship navigation function with respect to time. The ship navigator may make decisions to speed up or change route to stay on schedule. A major controlling aspect for ship navigation is to "Consider operational regulations." By considering these operational regulations, best practices, and guidance can be transferred to the ship navigator, helping to control the functionality. A precondition is that a ship must either be designed and/or procured and crew must be hired in order to navigate this ship. This is a precondition because it must happen prior to the ship navigation, but it does not initiate the ship navigation as the input does. The ship and crew can remain at port until the decision to leave port has been made, then "Navigate ship" can begin. Lastly, let's consider the resources necessary to navigate a ship. In the FRAM, resources should be focused on items that are consumed during or need to be resupplied after a function is executed. While, we could think of the ship as being a resource, it will not be consumed (at least not over a single voyage), and is more appropriately considered as a precondition aspect. Resources such as cargo and consumables (fuels, stores, ballast, maintenance materials) will be consumed during a voyage and should be resupplied before another voyage is to begin.

This generalized model (Figure 3.3) has helped us define scope and start thinking about ship navigation in terms of the FRAM. However, the model is not yet detailed enough to provide much useful insight. Now that the scope is better understood, the focus can be shifted to understanding how ship navigation is carried out.

3.5.2. Building a conceptualized FRAM model

In the FRAM, it is best to have your assessment informed by the workers who carry out or interact closely with the system functions. However, it is useful to first build a conceptualized model from the perspective of the assessors to help illustrate the FRAM to the worker(s) in the context of their operation. This conceptualized model can be seen in Figure 3.4.

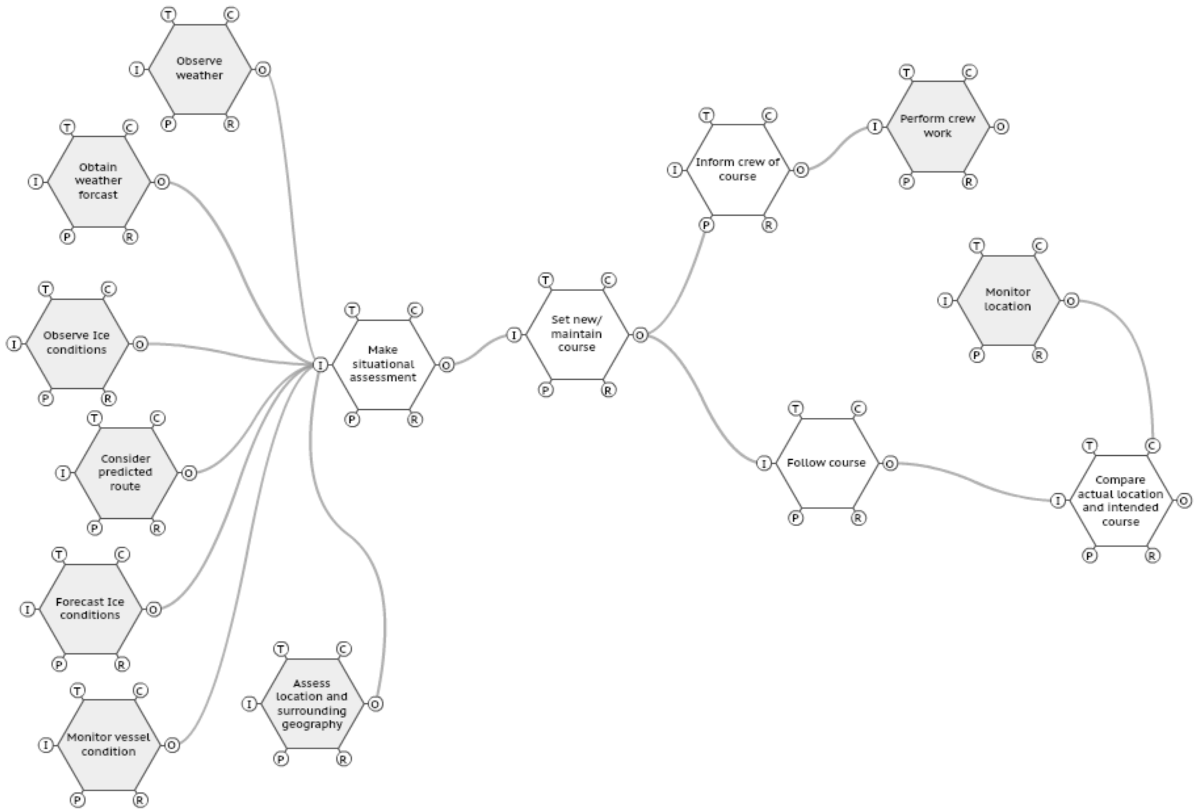


Figure 3.4: Conceptualized FRAM model for ship navigation

In Figure 3.4, the ship navigation process is described as a continual assessment of the conditions that result in a decision to maintain a course or to change course. This can be done many times over a single voyage. The decision then leads to the navigator following the chosen course and notifying the crew of any adjustments, if necessary. In order to reasonably make an assessment, the ship navigator must consider many conditions comprehensively to make the most informed decisions. The outputs from these functions may be produced at different rates and assessments by the navigator will be made with varying levels of information. Some of the inputs that we can imagine are important to a navigator's assessment are:

- Observing the current weather conditions
- Obtain weather forecasts
- Observe the ice conditions
- Obtain ice forecasts
- Consider the intended or predicted route
- Monitor the condition of the vessel
- Be aware of the surrounding location and geography

3.5.3. Verifying with workers

To inform our assessment, we spoke with three ship captains. The discussions were focused on understanding how ship navigators navigate ships, and making note of any unusual variations or conditions that they shared. The representation of ship navigation (Figure 3.4) was critiqued by the three ship navigators and it contained many of the functions that the navigators used but it was incomplete. Consider the functional descriptions and the initial description of the aspects for ship navigation in Table 3.1. The only times that an output will by omitted is when it has been left out to define the scope of the analysis. Similarly, when “not initially described” is listed, this does not mean that that aspect is not present. It means that the scope has initially been limited to describing the coupling of the immediate functions that have been described. This will help prevent becoming overwhelmed with complexity initially. Additional aspects can be further described later, if needed.

It can be seen that additional functions have been identified through conversations with ship navigators. The visual representation of the FRAM model with input from ship navigators can be seen in Figure 3.5. It can be seen that this more detailed description of ship navigation shows a more complex representation than the one in Figure 3.4. It is important to understand the complexities that are present in ship navigation because these complexities must be managed in the operation, whether we decide to model them or not.

Table 3.1: Initial description of FRAM functions and aspects for ship navigation

Name of function	Obtain weather forecast	Set new/ maintain course	Observe Ice conditions
Description	Obtain weather forecast from meteorological organization or department	A decision is made to either maintain the current course or to make adjustments to course.	Observe the current ice conditions. This can be done from the bridge or on deck, but also the conditions ahead can be observed via helicopter or aircraft
Aspect	**Description of Aspect**	**Description of Aspect**	**Description of Aspect**
Input	Not initially described	Complete or partial assessment made	Not initially described
Output	Weather forecast obtained	Routing decision made	Ice conditions have been visually observed onboard
			Up route ice conditions assessed with helicopter
Precondition	Not initially described	Not initially described	Not initially described
Resource	Not initially described	Not initially described	Not initially described

Control	Experience based weather judgement	Not initially described	Experienced visual assessment of ice Radar image observed
Time	Not initially described	Not initially described	Not initially described
Name of function	Forecast Ice conditions	Assess location and surrounding geography	Inform crew of course
Description	Obtain the forecasted ice conditions. This may be done by historical trends in area and/or tactical ice drift models	Locate the vessel with respect to intended route, shipping lanes and regional geographic features.	Inform crew of any change of course if necessary.
Aspect	Description of Aspect	Description of Aspect	Description of Aspect
Input	Not initially described	Not initially described	Not initially described
Output	Obtained forecasted ice conditions Daily ice chart observed	Geographical assessment made	Responsible crew member notified
Precondition	Not initially described	Aware of the present route	Routing decision made
Resource	Ice chart downloaded	Not initially described	Not initially described

Control	Experience based ice forecast	Have shipping lane maps Improved knowledge of regional specific conditions	Not initially described
Time	Not initially described	Not initially described	Not initially described
Name of function	Assess location and surrounding geography	Make situational assessment	Perform crew work
Description	Locate the vessel with respect to intended route, shipping lanes and regional geographic features.	The captain and bridge team make a situational assessment based on the available information at a given time.	The crew will perform their necessary work to maintain course or adjust their work to accommodate any changes.
Aspect	Description of Aspect	Description of Aspect	Description of Aspect
Input	Routing decision made	Weather forecast obtained Up route ice conditions assess. with Helicopter Obtained forecasted ice conditions	Responsible crew member notified

		Geographical assessment made	
		Weather has been observed	
		Aware of apparent vessel condition	
		Ice conditions have been visually observed onboard	
		Proximate traffic communicated with	
Output	Not initially described	Complete or partial assessment made	Not initially described
Precondition	Not initially described	Not initially described	Not initially described
Resource	Not initially described	Not initially described	Not initially described
Control	Not initially described	Ice Numeral computed	Not initially described
Time	Not initially described	Not initially described	Not initially described
Name of function	Observe weather	Consider predicted/updated route	Compute Ice Numeral

Description	The current local (ship) weather conditions are observed. This can be from the bridge or on deck.	Consider the current route you are transiting. This may be suggested by operational planners or adjusted by the navigator.	Compute the ice numeral as per Canadian regulatory requirements.
Aspect	Description of Aspect	Description of Aspect	Description of Aspect
Input	Not initially described	Not initially described	Daily ice chart observed
Output	Weather has been observed	Aware of the present route	Ice Numeral computed
Precondition	Not initially described	Not initially described	Ship classification assigned
Resource	Not initially described	Not initially described	Not initially described
Control	Not initially described	Not initially described	Not initially described
Time	Not initially described	Shipping schedule made	Not initially described
Name of function	Monitor vessel condition	Assign ship classification	Download daily ice charts
Description	The vessel's condition is monitored to understand the vessel's current capabilities.	The ship is assigned a classification. In particular, this classification here pertains to the category	Download the daily ice chart(s) that are applicable to your region. These charts are produced by Canadian

		that will be used to compute the ice numeral.	Ice Services (CIS) in Canada.
Aspect	Description of Aspect	Description of Aspect	Description of Aspect
Input	Not initially described	Not initially described	Not initially described
Output	Aware of apparent vessel condition	Ship classification assigned	Ice chart downloaded
Precondition	Engine room maintenance/issues informed	Not initially described	Not initially described
	Aware of vessel's typical capability		
Resource	Not initially described	Not initially described	Not initially described
Control	Not initially described	Not initially described	Not initially described
Time	Not initially described	Not initially described	Not initially described
Name of function	Ice navigator makes assessments	Obtain map of shipping lanes	Observe radar image

Description	Ice navigator makes assessments of the conditions and upcoming tasks and shares experience with ships bridge team.	Prior to shipping through an area it is good practice to obtain maps of the shipping lanes. The shipping lanes typically has more reliable soundings and have been practiced over the years.	The radar image is observed and then should be visually inspected to determine what caused the radar image to be produced
Aspect	Description of Aspect	Description of Aspect	Description of Aspect
Input	Not initially described	Not initially described	Not initially described
Output	Experienced visual assessment of ice Experience based ice forecast Improved knowledge of regional specific conditions Experience based weather judgement	Have shipping lane maps	Radar image observed
Precondition	Ice navigator has been assigned	Not initially described	A radar signal has been detected by ships radar

Resource	Not initially described	Not initially described	Not initially described
Control	Not initially described	Not initially described	Not initially described
Time	Not initially described	Not initially described	Not initially described
Name of function	Observe other traffic	Communicate with proximate traffic	Communicate with engine room
Description	Observe any other shipping traffic that may be in the area	Communicate with proximate traffic. This can be done via lights, horns or radio.	There is communication between the engine room and the bridge to discuss any issues or needed maintenance.
Aspect	Description of Aspect	Description of Aspect	Description of Aspect
Input	Not initially described	Other traffic observed	Not initially described
Output	Other traffic observed	Proximate traffic communicated with	Engine room maintenance/issues informed
Precondition	Not initially described	Not initially described	Not initially described
Resource	Not initially described	Not initially described	Not initially described
Control	Radar image observed	Not initially described	Not initially described
Time	Not initially described	Not initially described	Not initially described
Name of function	Assign certified ice navigator	Detect radar image	Become aware of vessel's capability

Description	To assign an ice navigator to assist with navigation of the vessel. This is required for Navigation in the Canadian Arctic.	Radar signal has been sent from ships radar and is ready to receive any signals that bounce back from objects	The navigator becomes aware of the vessel's capabilities. The navigational, structural and operational capabilities.
Aspect	Description of Aspect	Description of Aspect	Description of Aspect
Input	Not initially described	Not initially described	Not initially described
Output	Ice navigator has been assigned	A radar signal has been detected by ships radar	Aware of vessel's typical capability
Precondition	Not initially described	Not initially described	Not initially described
Resource	Not initially described	Not initially described	Not initially described
Control	Not initially described	Not initially described	Not initially described
Time	Not initially described	Not initially described	Not initially described
Name of function	Make shipping schedule		
Description	Expected departure and arrival times are determined.		
Aspect	Description of Aspect		
Input	Not initially described		

Output	Shipping schedule made		
Precondition	Not initially described		
Resource	Not initially described		
Control	Not initially described		
Time	Not initially described		

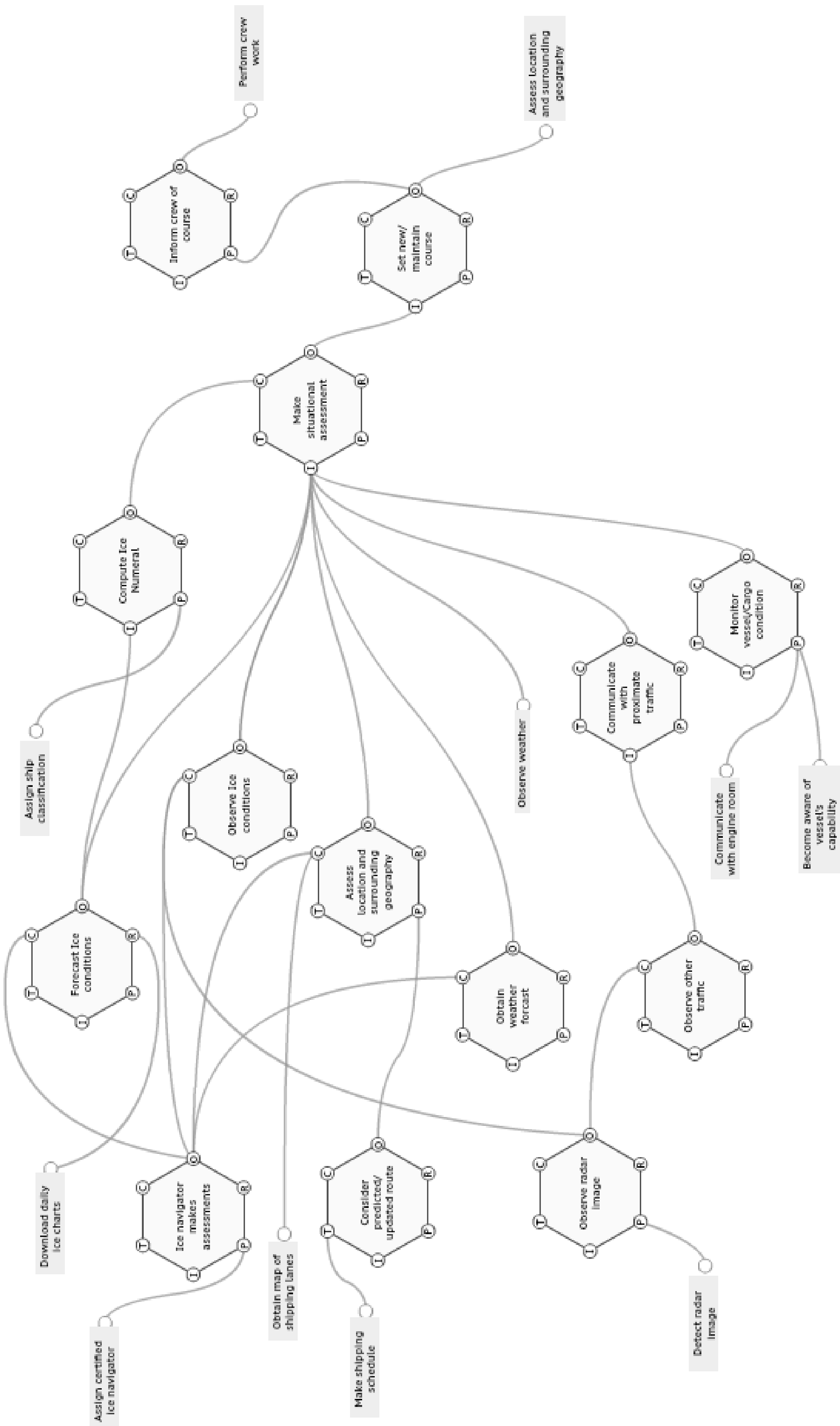


Figure 3.5: FRAM model for ship navigation with input from ship navigators

3.5.4. Learning Variations

Figure 3.5 shows a map of the potential ways that a ship could be navigated. But there are many ways the ship could be navigated, including combinations of the potential functional paths shown in Figure 3.5. This variability must be understood, if it is to be properly managed. Also, there will be more Arctic specific knowledge here, because Arctic ship navigation is a variation of ship navigation. See Table 3.2 for sources of variability and additional notes along with some ways this variability has been managed in the past. This model can help to better understand some shipping scenarios.

Table 3.2: Variability, notes and management strategies with focus on Arctic shipping

Associated Function	Sources of potential variability	Notes and Management techniques
Set new/ maintain course	More than one possible course	Slow down - allow time to receive more information - make more informed decision
	Scheduling and expected profits can influence decision making	
	The amount of consumable onboard also affect decision making (route selection)	
	GPS may not be accurate at high latitude	

Assess location and surrounding geography	Coastline and underwater mapping may be poor in areas of Arctic	
	Sounding could be inaccurate outside of shipping lanes	
Consider predicted/updated route	Possible multiple routes - NWP has 3	Dynamic set of solutions
	Ice conditions may take you outside of shipping lanes	
	Search and rescue operation can take you outside of shipping lanes	
Compute Ice Numeral		This is computed once daily - when a new ice chart is published.
		The computation is based on the ice assessment from the ice chart - If the chart contains errors it will affect the appropriateness of the computation
Detect radar image	Small icebergs (growlers) can be difficult to detect in ice	Reduce speed - increase reaction time if detected late

	Small icebergs (growlers) can be difficult to detect in large sea states	
	Dome shaped icebergs may be problematic to detect	
	Sleet can affect performance of radar	
	Quality of the installed radar technology	
Observe Ice conditions	Darkness affects ability to see ice conditions	Good searchlight - very valuable and backup searchlights
	Experience of Ice navigator and Captain	With uncertain conditions, reduce speed to minimize force of unexpected impacts
	Real conditions can be worse than was forecasted	Deal with it and/or turn around
	Ice charts are published 24 hours - over 24 hours the ice will move	Try to use ice chart and radar to predict ships position in changing ice field. Also send helicopter for visual inspection if available. Important to remember that ice moves with

		wind and icebergs will move with current
Forecast Ice conditions	Quality of Ice chart	Quality usually improves if aerial assessment of the region has been done
	Forecast models may be poor for certain regions	Experienced ice navigator can also provide experience based forecasts
Obtain weather forecast	Forecast maybe poor quality or non-existent for some regions of the Arctic	Experienced ice navigator can also provide experience based weather forecasts of local weather patterns
	How many weather forecasts are available daily?	
	Communications problems at high latitudes can affect ability to obtain forecast	
Observe weather conditions	Can observe variety of conditions - Wind and snow can affect visibility - Cold rain can expect icing	

	Notice differences from weather forecasts	Ice navigator may be able to help determine how weather might change
Make situational assessment	Is full bridge team present?	Other work commitments may take them from bridge when assessment is made
	How much time to make assessment	Can slow down to make more time
	Here is the function that influenced by all other analysis functions	Variations of every upstream function will influence the quality of the assessment here
	Fatigue can affect assessments and decision making	Shift schedules can affect fatigue - Ice-induced vibrations can affect fatigue
	Ice pressure can be problematic for ship navigation, even in low ice thickness	
	Longer periods of darkness can affect decision making	
	Slush has the potential to clog cooling water intakes, and risk losing engine - this has been seen in the past	Finer screen over water intakes

	Icebreaker assistance may be called for if conditions become unmanageable for vessel. This could take some time if not planned for in advance	When following/being towed by icebreaker: Keep prop turning, May have to follow very closely in high ice pressure field (channel will close in). Use ice to help stop when following closely (prevent collision)
Communicate with engine room	Communicate upcoming maintenance	Work culture may influence communication frequency
	Communicate performance issues	
Monitor vessel condition	Wet conditions or open water can promote marine icing	Breaking off the ice can also be a dangerous procedure and is usually avoided until absolutely necessary
	There are icing allowances in stability book	It is very difficult to monitor the weight of ice buildup and distribution of the weight
	Parallel mid-body stress will be high if entering a mobile ice field from fast ice (shear zone)	Avoid if possible

	Difficult to monitor (feel) bow impacts if bridge is positioned astern	
	Backing up in ice	Keep rudder straight when moving astern
Perform crew work	Crew may not be prepared for and have experience in cold climate	

3.6. Discussion

It is important to understand that this model still has missing elements. It can be expanded to incorporate more elements to improve our understanding of socio-technical system that is ship navigation. It is acknowledged that there are regulatory functions and organizational functions omitted from this model. These functions are carried out at lower frequencies than the onboard functions, but will influence the onboard work. The next step is to better understand how these regulations and organization affect the functionality of ship navigation. It may be also appropriate to further define some functions. For example, it may be appropriate to break down the “Monitor vessel condition” function into separate functions, as in Figure 3.6.

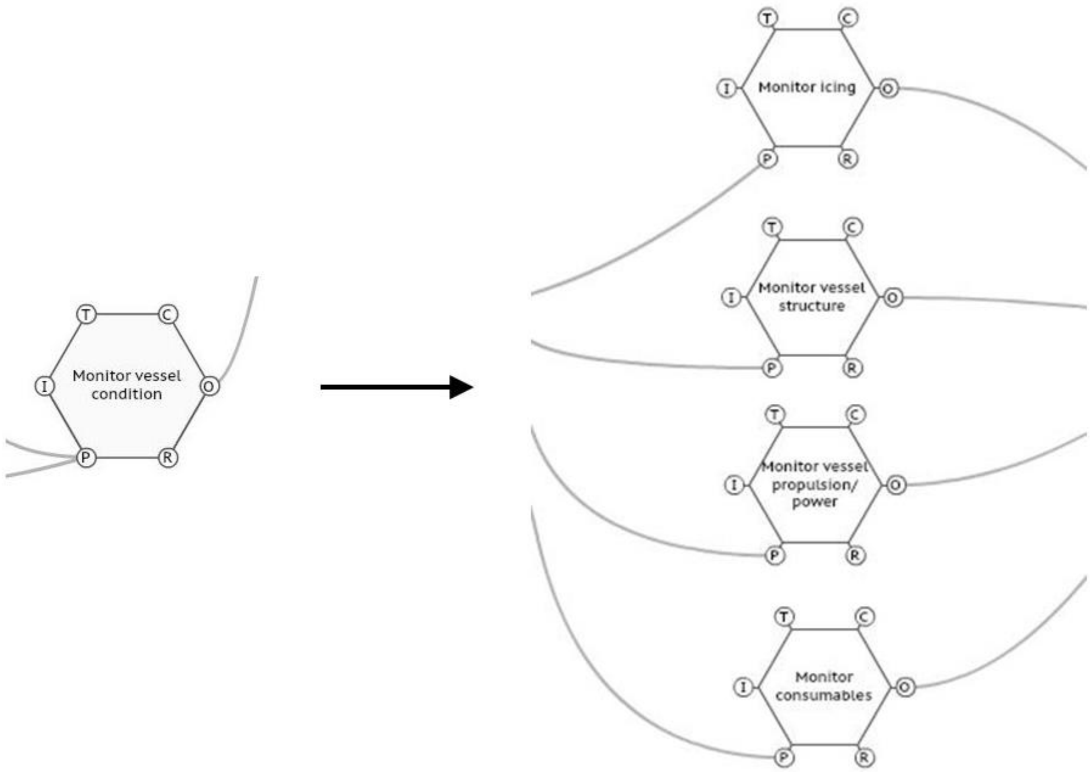


Figure 3.6: Breaking function into sub-functions

Then it may be appropriate to ask: 1) when is the FRAM model "complete"? and 2) How do we know if we have sufficient granularity? The model will never be complete but each revision should improve the understanding. There is no guarantee that future operations will mirror past operations, so there are always new lessons to learn. As long as the system is operating, there will be new information to add to your FRAM model. It will depend on what you are trying to explain and the explanations you are willing to accept. The detail of the function may be acceptable to explain one scenario, but inadequate to explain another. In this case, it is important to not try to categorize explanations into two discrete groups, right or wrong. Explanations can range from poor to acceptable, and further examination will produce better explanations. As more details are understood acceptable explanations will emerge. The question then becomes, what is acceptable? Explanations should be sought that not only describe what happened, but how it happened and why it happened. By understanding these 3 parts of a scenario, better management strategies will be able to be developed.

In order to demonstrate the utility of this information, it should be used to explain certain scenarios from the shipping domain. The FRAM model can be used to add to the understanding that have been obtained from traditional examination techniques. In section 3.6.1 the Exxon Valdez case will be considered.

3.6.1. Applying a case: the Exxon Valdez grounding

The Exxon Valdez grounded on March 24, 1989 on Bligh Reef in Prince William Sound while transporting crude oil from Valdez, Alaska to San Diego, California. This shipping accident is one of the most well-known, which garnered much media attention and legal intervention because of its environmental impact and ill-defined oil spill response policy. In terms of Arctic shipping accidents, the Exxon Valdez case is the most well documented accident that is publicly available. This case may be the most suitable case to examine through the lens of the FRAM because of the extent of information available compared to other cases.

All information in this case is taken from the National Transportation Safety Board's (NTSB) marine accident report on the Exxon Valdez accident (NTSB, 1990). The NTSB performed an extensive investigation and analysis of this accident. The report included 47 findings that were determined to be relevant to the accident, an account of probable cause, and recommendations to the organizations/departments involved. The report has been a very significant document for shipping safety and influenced the adoption of double hull tankships across the industry. The adoption of double hull tankships has improved safety of the tankship industry, specifically with respect to its relationship to the environment.

The account of probable cause is as follows (NTSB, 1990):

"The National Transportation Safety Board determines that the probable cause of the grounding of the EXXON VALDEZ was the failure of the third mate to properly maneuver the vessel because of fatigue and excessive workload; the failure of the master to provide a proper navigation watch because of impairment from alcohol; the failure of Exxon Shipping Company to provide a fit master and a rested and sufficient crew for the EXXON VALDEZ; the lack of an effective Vessel Traffic Service because of inadequate equipment and manning levels, inadequate personnel training, and deficient management oversight; and the lack of effective pilotage services."

This account of probable cause can be visualized by the causal dependency diagram in Figure 3.7.

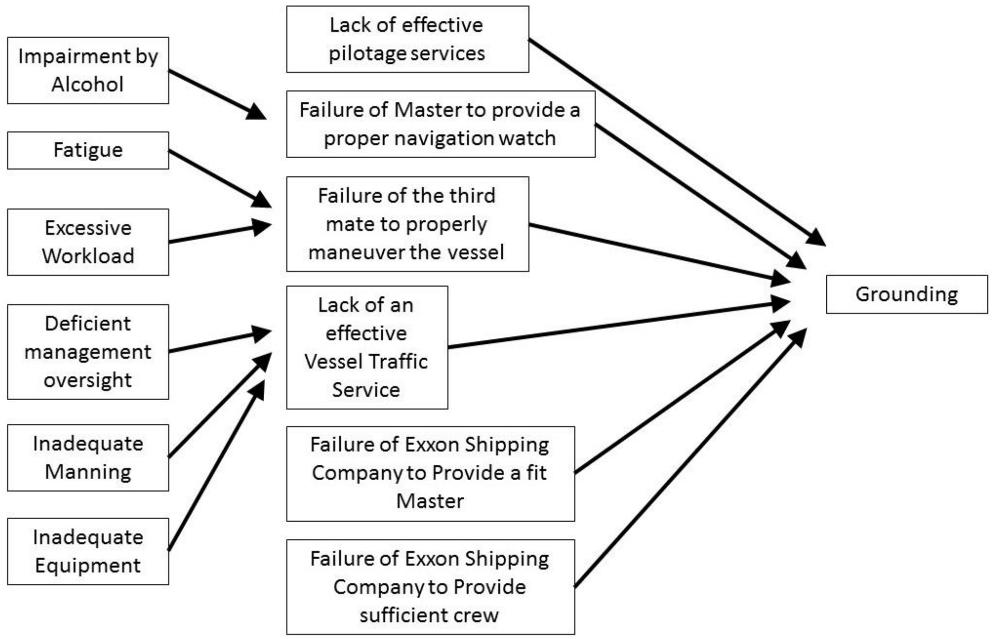


Figure 3.7: Causal dependency diagram produced from the account of probable cause given in the Marine Accident Report

Now consider how the grounding would look by applying the information in the grounding report to the FRAM model for Arctic ship navigation. The FRAM model shown in Section 3.5.3 displays the potential functional paths to navigating the vessel. The Exxon Valdez case can be used to illustrate the functional dynamics that contributed to the grounding. The generalized FRAM model seen in Figure 3.5 represents the potential ways that an Arctic ship navigator could operate the ship. However, when a ship navigator operates the vessel, many combinations of selected functions may be used. The marine accident report of the Exxon Valdez grounding can be used to help understand the functional dynamics that occurred during that accident (NTSB, 1990).

Appendix C shows the functional signature of the Exxon Valdez voyage from 21h21 on March 23, 1989 up until the time of the grounding. It should be noted that some of the times are estimated based on the accounts given in the Marine Accident report and the actual time may vary slightly from the time stated in this analysis. Each figure represents a snapshot of the active functions at a stated time for the Exxon Valdez grounding. The collection of these snapshots represent the functional signature of the Exxon Valdez grounding.

Figure 3.8 shows that at about 23h55 on March 23, 1989 the Navigator (Third Mate) and his team were assessing the location of the Exxon Valdez relative to Busby Island Light to determine if it was time to turn back towards the shipping lane that they had left to avoid glacial ice. At this time, the navigator was using the radar to estimate the vessel’s position from Busby Island Light, which he estimated to be 0.9 miles away. Also, a fix was plotted on a chart of the vessel’s position from visual observations, which estimated Busby Island Light to be 1.1 miles away. There was a discrepancy of 0.2 miles of the navigator’s estimates of the vessel’s position. Additionally, during this functional snapshot there was an additional functional relationship learned that existed between observing the radar image and assessing the vessel’s location and surrounding geography. This relationship was not noticed in previous discussions with ship captains and was added to the model (one of the blue lines in Figure 3.8) to add to the model’s comprehensiveness.

In this analysis, the functional signature of the Exxon Valdez was presented. This represents a single voyage for this vessel. From this data alone, it is difficult to determine with high certainty what caused this accident. However, if there was data available about other voyages that the Exxon Valdez had and successfully navigated through Valdez Narrows, there would be a better understanding of the functional signatures that promoted better performance of the Exxon Valdez. Presumably, the vessel successfully navigated the

Narrows before while the captain was away from the bridge, while workers were fatigued, or while glacial ice entered into the shipping lanes. By using a method that is capable of also analyzing successful voyages, there is a better chance of identifying what was different about the functional signatures that promote such different outcomes. Additionally, if this information was available, the value of this analysis could be increased.

By considering systemic safety solutions and understanding the navigational processes, additional safety recommendation can be made. For instance, in addition to recommending minimizing fatigue by analyzing ideal shift schedules, elements could be introduced into the system that help navigators perform better even when fatigued. It can be reasoned that even under ideal sleeping conditions, e.g. a person working a 9-5 desk job, a person can arrive at work tired or fatigued. Additional recommendations of updating the autopilot system to be more evident as to when it was engaged or disengaged, as this was a source of confusion for the crew of the Exxon Valdez during the grounding. This could help fatigued workers be more aware of the condition of their vessel. Additionally, other technologies could be recommended that help ship navigators more accurately assess their location in a waterway. In the present, the addition of GPS on vessels may help with this although, some of the Captains consulted in section 3.5.3 have expressed concern about GPS accuracy at high latitudes.

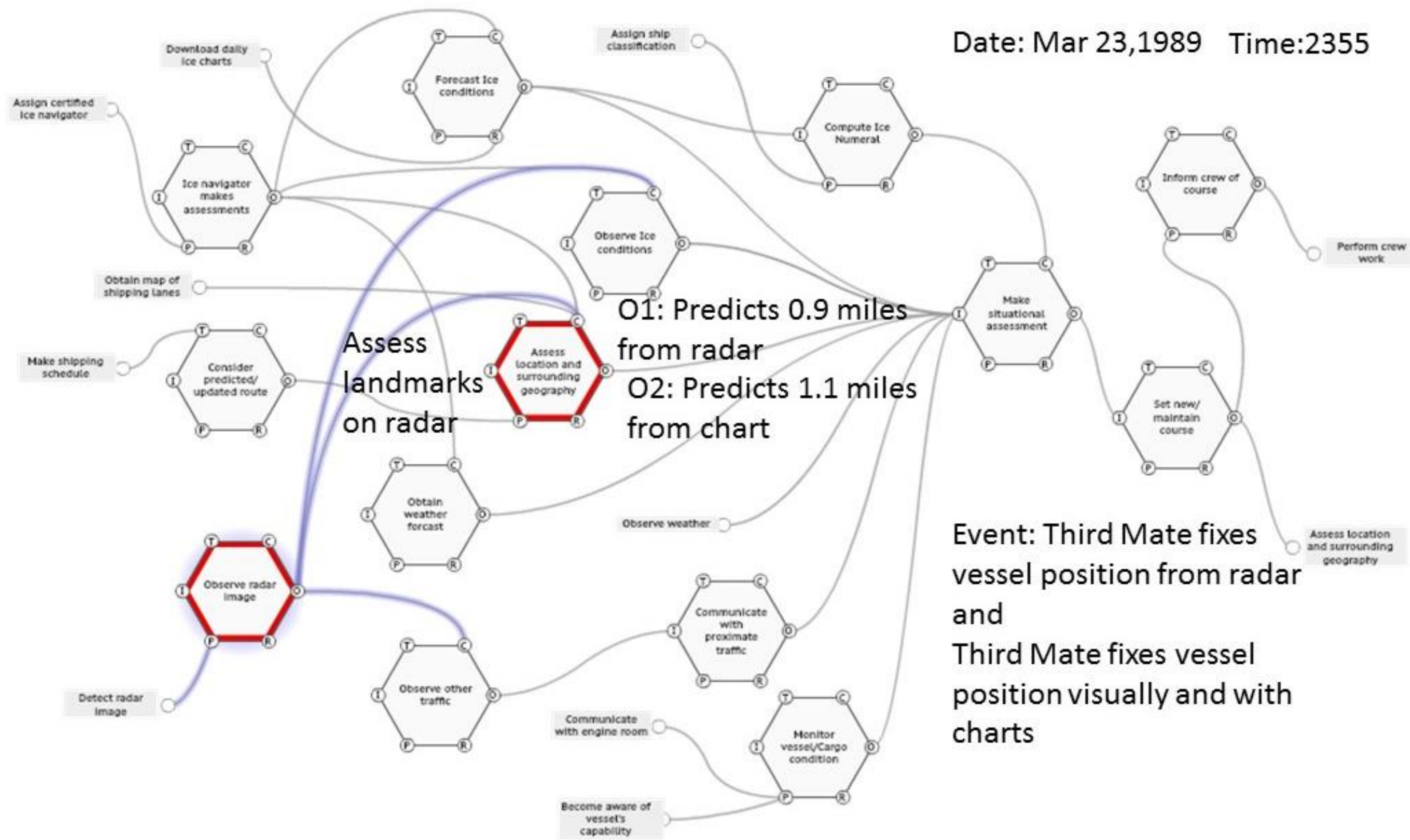

Date: Mar 23,1989 Time:2355
Event: Third Mate fixes vessel position from radar
and
Third Mate fixes vessel position visually and with charts
O1: Predicts 0.9 miles from radar
O2: Predicts 1.1 miles from chart
Assess landmarks on radar
Download daily ice charts
Assign certified ice navigator
Forecast Ice conditions
Ice navigator makes assessments
Assign ship classification
Compute Ice Numeral
Inform crew of course
Perform crew work
Observe Ice conditions
Obtain map of shipping lanes
Make situational assessment
Assess location and surrounding geography
Make shipping schedule
Consider predicted/ updated route
Set new/ maintain course
Obtain weather forcast
Observe weather
Assess location and surrounding geography
Observe radar image
Communicate with proximate traffic
Detect radar image
Observe other traffic
Communicate with engine room
Monitor vessel/Cargo condition
Become aware of vessel's capability

Figure 3.8: Functional representation of the Exxon Valdez grounding at about 23h55 with updated functional relationship (blue lines)

3.7. Conclusions

In this work, the FRAM has been used to start an investigation into Arctic shipping by trying to understand ship navigation and its variations in ice. The process of building a FRAM model was discussed and an application of the model was illustrated using the Exxon Valdez grounding. After speaking with the ship navigators, a more detailed FRAM representation of ship navigation has been developed. Some of the variations and conditions that are present in Arctic navigation are discussed along with the ways that ship navigators manage these conditions. The grounding of the Exxon Valdez was examined and provided context to the information that was made available by the Marine accident report. This case allowed for an alternative perspective and complementary discussion of the case than could have been had without the FRAM.

It is acknowledged in this work that there are still elements that factor into the ship navigation process that are omitted for now, including many regulatory functions and organizational functions. This work serves as an initial starting point to use the FRAM to help better understand the complexities that exist for ship navigation in the Arctic. This work can be improved in the future by further defining the functional descriptions, incorporating more variations that have been experienced, and extending the scope of the assessment. The framework to do this is presented in this paper and new information can be used to update the model.

3.8. Acknowledgements

The financial support of the Lloyd's Register Foundation is acknowledged with gratitude. Lloyd's Register Foundation helps to protect life and property by supporting engineering-related education, public engagement and the application of research.

3.9. References

Arctic Council, 2009. Arctic Marine Shipping Assessment 2009 Report.

Aven, T., Andersen, H.B., Cox, T., Droguett, E.L., Greenberg, M., Guikema, S., Kröger, W., Renn, O., Zio, E., 2015. Risk Analysis Foundations. Soc. Risk Anal.

Ayyub, B.M., 2015. Practical Resilience Metrics for Planning, Design, and Decision Making. ASCE-ASME J. Risk Uncertain. Eng. Syst. Part Civ. Eng. 1. doi:http://dx.doi.org/10.1061/AJRUA6.0000826

Ayyub, B.M., 2014. Systems resilience for multihazard environments: definition, metrics, and valuation for decision making. Risk Anal. Off. Publ. Soc. Risk Anal. 34, 340–355. doi:10.1111/risa.12093

Borys, D., Else, D., Leggett, S., 2009. The fifth age of safety: the adaptive age. J. Health Saf. Res. Pract. 1.

Hollnagel, E., 2012. FRAM: The Functional Resonance Analysis Method. Ashgate Publishing Ltd.

Hollnagel, E., Woods, D.D., Leveson, N., 2006. Resilience Engineering: Concepts and Precepts. Ashgate Publishing Ltd., Hampshire, UK.

Leveson, N., 2004. A New Accident Model for Engineering Safer Systems. Saf. Sci. 42, 237–270.

NTSB, 1990. Marine Accident Report - Grounding of the U.S. Tankship EXXON VALDEZ on Bligh Reef, Prince William Sound, near Valdez, Alaska, March 24, 1989 (No. NTSB/MAR-90/04). National Transportation Safety Board, Washington, D.C.

Smith, D., Veitch, B., Khan, F., Taylor, R., 2015. An Accident Model for Arctic Shipping, in: Proceedings of the ASME 2015 34th International Conference on Ocean, Offshore and Arctic Engineering. Presented at the OMAE 2015, St. John's, NL, Canada.

Vicente, K., 2004. The Human Factor: Revolutionizing the Way People Live with Technology. Routledge, New York.

4. INTEGRATION OF RESILIENCE AND FRAM FOR SAFETY MANAGEMENT

4.1. Co-authorship statement

A version of this manuscript has been submitted for publication in the ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering and is currently under a second peer-review process. The manuscript was written by authors, Doug Smith, Brian Veitch, Faisal Khan, and Rocky Taylor. Author Doug Smith led the writing of this manuscript, including development of the methodology, the discussion of this method, development of the FRAM model and functional signatures for driving a car to work. All authors revised, edited, discussed this work and made recommendations for improvements to its presentation.

4.2. Abstract

Resilience is a concept that can be used to bring additional understanding to safety management, to complement traditional approaches. The additional understanding will enable more informed safety management decisions to be made by operators. This is critical for operations in remote and hash environments. The concepts of resilience, such as robustness and rapidity, can be used to inform safety management decisions. A methodology is presented that uses quantitative techniques of system performance measurement and qualitative understanding of functional execution from the Functional

Resonance Analysis Method (FRAM) to gain an understanding of these resilience concepts. Examples of robustness and rapidity using this methodology are illustrated, and how they can help operators manage their operation is discussed.

Keywords: Resilience, FRAM, Safety Measurement, Safety System

4.3. Introduction

Risk management is an important part of industrial applications and paramount to the success of businesses. Risk is characterized by the probability of unfavorable events occurring and the magnitude of their consequences. A fundamental principle of risk is the Law of Large Numbers. This says that given a large enough sample size, the expected value will converge to its true probabilistic value. But this principle has no bearing on what will happen in a single sample. That is why safety assessors must actively monitor operations, try to understand precursors to foresee single outcomes as they emerge, and so avoid unfavorable ones.

Many modern work places involve complex operations with many hazards appearing in dynamic environmental conditions. This makes it very difficult to foresee outcomes prior to commencing the operation. We rely on operators to actively assess and avoid many of the hazards that can and will occur during operation. This expertise is a source of resilience, which brings the operation success most of the time. Occasionally accidents do occur and blame for those accidents is attributed to human error 70-90% of the time (Rothblum, 2000; Shappell & Wiegmann, 2004; U.S. Department of Energy, 2009). Most of the time, humans are also the reason operations are successful (Hollnagel, 2014). By understanding the human element of operations better, there is an opportunity to manage the operation in a way that increases the resilient capabilities of humans, thus minimizing the risk of errors. Methods have been proposed to consider technical and human elements of complex socio-technical systems together (Hollnagel, 2012; N. Leveson, 2004; Vicente, 2004). These methods are systemic approaches that focus on modeling technical, organizational, and human factors together. By modeling these three factors together, an understanding can be obtained of the complex and adaptive nature of modern industrial operations (Borys et al., 2009). Adaptation to complex system dynamics reflects the resilience, which should be understood to help better inform safety management decisions.

In this paper, a methodology is presented that uses quantitative techniques of system performance measurement and qualitative understandings of functional execution from the Functional Resonance Analysis Method (FRAM) to evaluate resilient capacities of an industrial operation and inform safety management decisions. This methodology will help bring quantitative and qualitative understandings of resilience together, which has been a point of contention in the past. The quantitative part will provide a means to measure and evaluate, while the qualitative part will help provide an understanding of the mechanisms that produce certain performance measurements.

4.4. Background

4.4.1. Resilience

Resilience is a term that has garnered many definitions in various domains. Manyena (2006) compiled definitions of resilience from sources published from 1991 to 2005. Over the 14 year period, it was noted that definitions of resilience have evolved from an outcome, to a process that gives rise to an outcome. Another review of resilience definitions by Ayyub (2014) concluded that the term resilience was elastic in nature, which could possibly explain some ambiguity associated with the term. Definitions vary in level of detail, which can be seen in the two following examples, illustrating a vague definition and more detailed one, respectively: 1) The ability of an actor to cope with or adapt to hazard stress (Pelling, 2003); 2) the capacity of a system, community, or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure. This is determined by the degree to which the social system is capable of organizing itself to increase this capacity for learning from past disasters for better future protection and to improve risk reduction measures (UNISDR, 2005).

A common theme in more recent definitions of resilience is the reference to a system's ability or capacity rather than to an outcome. Béné et al. (2016) propose that resilience emerges from 3 capacities: absorptive, adaptive, and transformative. Each capacity leads to a different outcome: persistence, incremental adjustments, and transformational responses, respectively. This framework also proposes that the intensity of the shock/stressor applied to the system will determine the capacity that will allow the system to cope. For low intensity stressors, the system may use either absorptive, adaptive, or transformative capacities to cope, with preference being given to absorptive capacities that exhibit system stability. For moderate intensity stressors, the system may use either adaptive or transformative capacities to cope, with preference being given to adaptive capacities that exhibit system flexibility. For severe intensity stressors, the system may be left with transformative capacities to cope, which would signal that system changes need to be made.

While the definitions of resilience in current literature leave some ambiguity, certain techniques can be used to inform operators of resilient qualities that may exist. Park et al. (2013) stated that resilience is better understood as an outcome of a recursive process that includes sensing, anticipation, learning, and adaptation, making it complementary to risk analysis and valuable for adaptive management of complex, coupled engineering systems. By monitoring a recursive process of an industrial application, some of the resilient capacities of an operation can be understood. This understanding can help improve safety management strategies for operators.

Current understandings of resilience produce definitions that collectively exhibit elasticity, which makes monitoring difficult for such an ill-defined parameter. While it is difficult to monitor resilience directly, other system parameters can be monitored to improve the understanding of resilient capacities that might exist. Monitoring the system’s performance recursively can be useful to gaining insight to an operation. As system performance is a context specific parameter, it should reflect the requirements or objectives of the operation (Ayyub, 2014).

Using system performance as a signal to monitor resilient capacities can provide insight into the persistence of a system. Persistence describes the system’s ability to endure and recover from events. More specifically, monitoring system performance can improve the understanding of an operation’s robustness and rapidity. Robustness considers a system’s performance during an event with respect to its initial or expected performance. Events that produce measurements that signal low robustness may also indicate vulnerabilities in the operation. Rapidity describes the system's recovery with respect to time, an indication of how quickly the operation will bounce back after a loss of performance.

To monitor system performance, the method suggested by Ayyub (2015) can be used, as seen in Figure 4.1. System performance is almost always variable, so it can be monitored continuously on a performance spectrum, rather than as binary states of acceptable and not acceptable. Tracking the performance over time with respect to a defined datum will allow for monitoring of the system's resilient capacities. In Figure 4.1, system performance is measured as a percentage of the system's expected performance. In practice, the metric could be adjusted to reflect the main objective of the system.

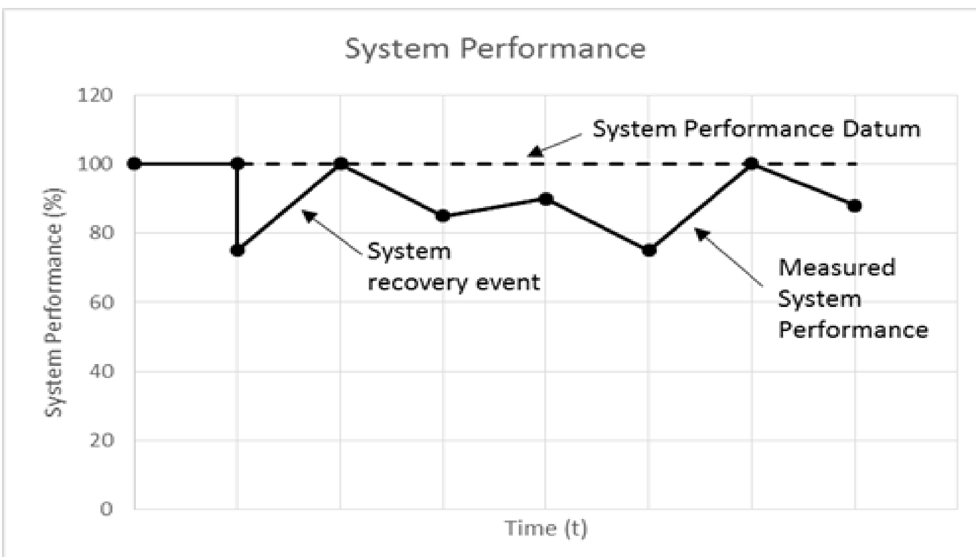


Figure 4.1: Measuring system performance over time

By monitoring system performance, some of the resilient properties of a system can start to be understood. Monitoring the system's overall performance can help understand robustness and rapidity of the operation. How robust the system is and how rapid the system recovers can be understood by the recursive monitoring of a system's performance over many events. This is an important step in operational management, which gives an appreciation of how the operation may respond to events. Monitoring system performance alone does not provide much insight to what system elements give rise to robustness and rapidity (or lack thereof) for the operation. Identification of the system elements that contribute to these resilient abilities can be useful for safety management. The Functional Resonance Analysis Method (FRAM) can be used to track the functional dynamics of an operation that give rise to the system performance measurements. Monitoring the functional dynamics and measuring the system's performance together can help identify these system elements.

4.4.2. FRAM

The FRAM is a method that produces a functional model. The model contains two main parameters: functions and variability. The functions should first be mapped to describe the potential functional pathways that are available in an operation, and provide an understanding of the connectivity of the work in that operation. The variability characterizes the variable nature of functional outputs and functional pathways that are actually taken in the operation. By modeling the system functions and variability in sufficient detail, valuable insights may emerge that can help inform safety management of complex operations.

The FRAM is based on four underlying principles (Hollnagel, 2012):

- Failures and successes are equivalent in the way that they happen for the same reason. Alternatively, it can be said that things go wrong for the same reasons that they go right.
- Daily performance of socio-technical systems, including humans individually and collectively, is always adjusted to match the system conditions.
- Many of the outcomes of the system that we notice, and the ones we don't notice, are emergent rather than resultant.
- Relations and dependencies must be described as they develop in a situation and not as cause-effect links. This is done through functional resonance.

The first step of the FRAM is to describe the functions of the system and the aspects of the functions that occur when work happens. Each function can have six aspects that should be considered in the model, as shown in (see Figure 4.2) (Hollnagel, 2012).

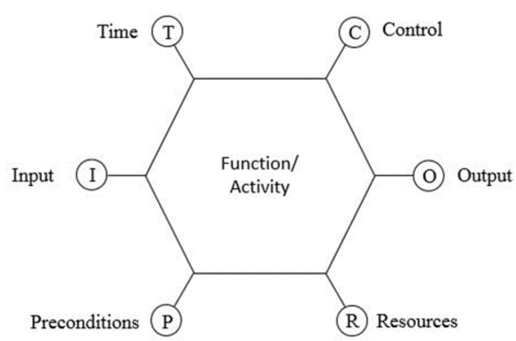


Figure 4.2: FRAM function diagram (Hollnagel, 2012)

The six aspects that should be considered include:

1) **Output**: Each function should have an output(s). If work is being done, there should be something produced by the work. The outputs are then passed throughout the system and have the potential to affect other work in the system in up to five ways.

2) **Input**: The input starts the functions. If the input is an output that arrives late from another function, it will affect the functionality of the downstream function.

3) **Preconditions**: Preconditions must be available prior to the function starting, but they do not initiate the function. They can lay dormant in the system until the function begins.

4) **Resources**: These are processed during the function. To limit the resources that are considered, focus should be on resources that are consumed and need to be resupplied by another function in the system.

5) **Time**: Other functional outputs have the potential to affect the available time to carry out a function.

6) **Control**: Other functions may interact with a downstream function in a way that acts as a control.

After the system's functions and aspects are described at some level of detail, the variability should be considered. Step 2 is to consider the internal variability of the function and the variety of ways an output can be produced under dynamic conditions. Step 3 is to assess the coupled system variability: the way the variations from upstream functions can affect the downstream functions and, in turn, the entire system performance. The final step is to identify appropriate ways to monitor the system and control the variability in it. In practice, it is very difficult to obtain all the necessary information at once and this process may need to be repeated as new information is obtained.

In practical terms, building the FRAM model provides an understanding of the potential ways that an operation could succeed. The variability provides an understanding of the ways that an outcome of the system is achieved, including both successes and failures. Variability can be examined in two ways: 1) as a variable signal of an output of single and combined functions, and 2) the variable functional paths that produce an outcome of the system. This variability can be tracked at a time step of the operation as seen in Figure 4.3, with labeled outputs of the variability of individual functions for that time step, and highlighted functions that show the active functions for that time step. This can also be stored in tabular form in a database. The monitoring of the particulars of variability of a given event produces a functional signature for that event.

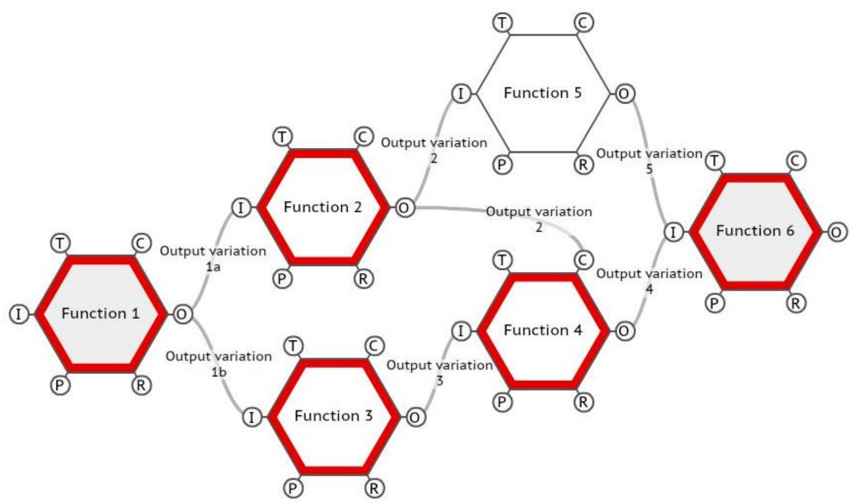


Figure 4.3: A variation of work functions for a given time (t)

4.5. Methodology

Well informed safety management decisions should be made using the most comprehensive knowledge possible. In the past, applications of resilience to safety management have been either quantitative or qualitative. The methodology presented here helps bring quantitative and qualitative knowledge together to better inform safety management decisions.

Quantitatively, system performance monitoring can help operators evaluate the variable performance of an operation. Over time, the performance of the operation due to dynamic conditions can be understood. This will first help to characterize the range and frequency of system performance values that are measured, then operators can have discussions regarding the need or opportunity to improve system performance. Additionally, by connecting the functional signatures of an operation to each system performance measurement, understanding of the system elements that contribute to resilient capacities can be gained. This understanding of the overall effect on the system's performance, combined with the understanding of the contributors to that performance, can help operators more effectively manage their operation.

Figure 4.4 displays a methodology for using resilience concepts and FRAM to understand and manage complex operations. This involves monitoring the system's performance and its corresponding functional signatures. Once system performance measurements and their functional signatures are collected, the measurements can be grouped into bins of similar levels of performance. For example, the measurements collected between 95%-100% system performance could be grouped together, as a high performance group. This group can be examined and compared to the other measurements. It can then be examined if the high-performance group exhibits any unique functional signatures. If so, those unique features may allow managers to incorporate them into more operations to promote higher performance more regularly. These unique features are functional contributors that contribute to a level of performance that falls within the grouping range. However, the identification of functional contributors is dependent on the number of cases examined and the content of those cases. Functional contributors may not always be identifiable during each examination, rather they may emerge as certain information is seen through the monitoring process. When functional contributors of certain performance levels are identified, operators can use the quantitative and qualitative understanding to manage their operation appropriately.

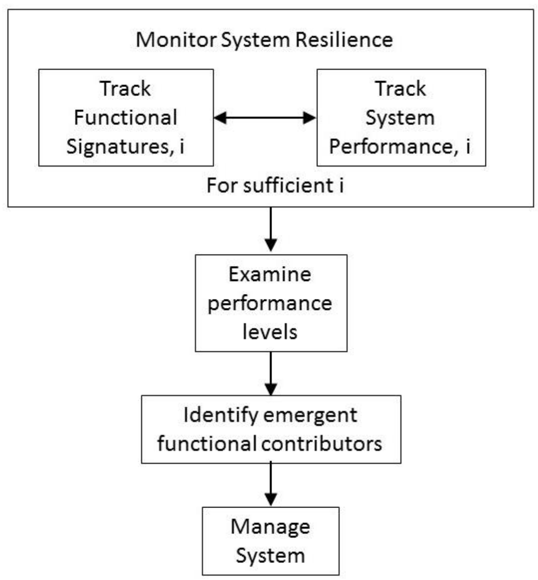


Figure 4.4: Methodology for managing system resilience

This methodology provides a framework to help bring a better understanding of resilience to operators and enable them to manage the system by bringing additional insights regarding resilience to their operation. The method adds opportunities to learn from successful operations, as opposed to more traditional methods that focus on failures to inform safety and operational management. The method uses performance measurements, as seen in Figure 4.1, and corresponding functional signatures, as seen in Figure 4.3, for each performance measurement to monitor the operation. As samples of the functional dynamics and performance measurements are collected, a range of performance levels can then be examined. The performance levels can be categorized into groups of high and low performance, or sliced into as finely or as coarsely as the examiner would like to investigate.

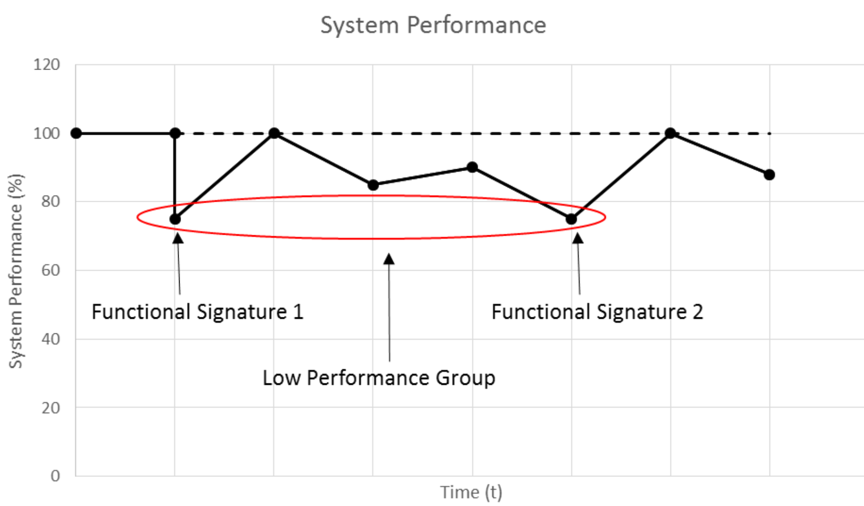


Figure 4.5: Examining low performance system measurements

The performance level can be defined as seen in Figure 4.5 by grouping low performance system measurements together. The functional signatures of the low performance group should be compared to all other functional signatures for the remaining measurements. Trends may emerge for functional contributors that produce low performance measurements, as opposed to higher performance measurements. This information will allow operators to manage out low performance measurements due to the identified functional contributor, which would increase robustness.

Additionally, the performance level could be grouped into high performance measurements, as seen in Figure 4.6. By comparing the functional signatures of the high-performance measurements to the functional signatures of the remaining performance measurements, trends may emerge for the functional contributors that produce high performance. This information can be used by management to promote high performance of their operation, which would also increase robustness.

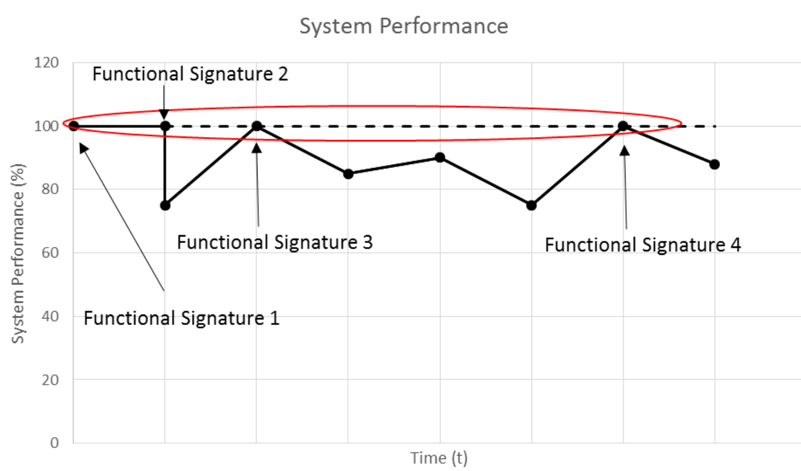


Figure 4.6: Examining high performance system measurements

Another resilient capability is the system's ability to recover after a loss of performance, which is rapidity. By grouping measurements that exhibit increasing system performance together, as seen in Figure 4.7, understanding of the operation's rapidity can be gained. By monitoring the system's functional signatures over the recovery, information will emerge regarding the system's rapidity. This information can help managers promote faster recovery after low performance measurements are seen.

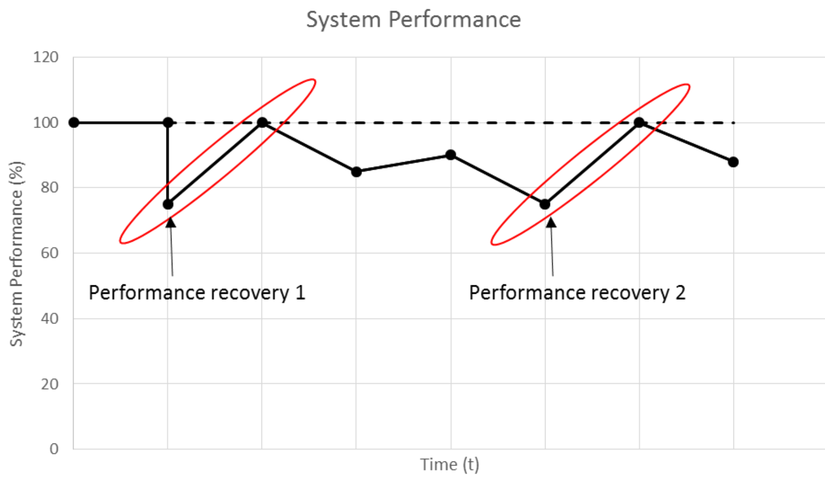


Figure 4.7: Examining system rapidity

The identification of functional contributors is emergent because the understanding of the contributors may not be evident after every examination of the system. As more samples are taken under various operational conditions, the functional contributors may emerge. Also, once the functional contributors start to emerge, the greater the number of samples that are seen will provide more evidence of a given contributor's impact on the operation. More evidence of the operational impacts of a functional contributor will help support a manager's decisions regarding the operation.

4.6. Discussion

In order to enrich the understanding of this method, it will be demonstrated using an easily relatable example - driving a car to work. The data presented in this example is hypothetical, but should serve to convey the application of the method. In order to track functional signatures, a functional model must be created. To track system performance, a performance metric must be determined.

A performance metric should capture the main objective of the operation, which for driving to work is to get you to work on time. Monitoring if you get to work on time or not would be binary and not show any difference in performance whether you were 1 minute late or 1 hour late. In order to capture these specifics of the operation it would be better to measure the time it takes to drive to work. It may also be useful to reference that metric against a performance datum to observe if the measured performance is approximately close to an expected level of performance. In this example, it is assumed that 25 minutes is a reasonable time to drive to work. This will be used as the performance datum and the metric will then be given as a percentage of system performance as shown in Equation 4.1.

$$\frac{Expected\ time\ (\text{mins})}{Measured\ time\ (mins)} \times 100\% = \frac{25\ mins}{Measured\ time\ (mins)} \times 100\% \qquad (4.1)$$

To build a functional model the FRAM can be used. The FRAM provides guidelines for building the functional model. The FRAM asks the assessor to describe the functions involved in the operation and the relations between the functions. This description will serve as a functional model. Figure 4.8 shows the FRAM model for driving a car. In practice, it would be wise at this stage to exercise the model, make observations of the operation you are modelling, and check that they are consistent with the model. However, in this hypothetical example it will be assumed that this version of the model is valid.

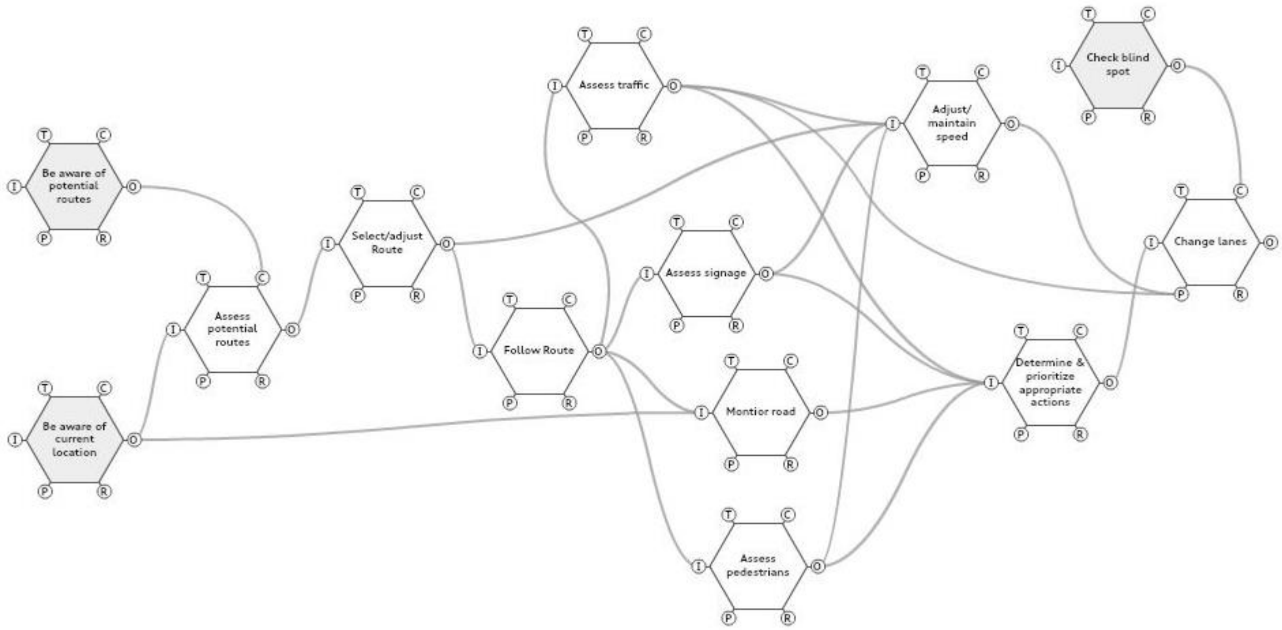


Figure 4.8: FRAM model for driving a car

This model shows the potential functions that could be executed while driving a car. Actually, this model describes the potential functions that could be executed to make driving decisions based on monitoring information and selecting/following routes. The model may repeat itself many times over a drive to work. Anytime you drive to work the outputs of the functions may be variable and only a portion of the functions may be used at specific times. This reflects the variability element of the FRAM and by tracking these variable processes over time a functional signature of the event can be captured.

Now that the metric has been defined and the functional model has been built, the operation can be monitored to understand the performance being achieved and the processes that are leading to certain levels of performance.

Suppose that over a period of time the system performance was measured for each drive to work. The hypothetical performance is displayed in Figure 4.9. These measurements give a sense of the level of performance being achieved in the operation and the variability in performance. Figure 4.9 alone does not provide much insight as to why certain levels of performance are occurring. To help gain this insight, functional signatures can be used.

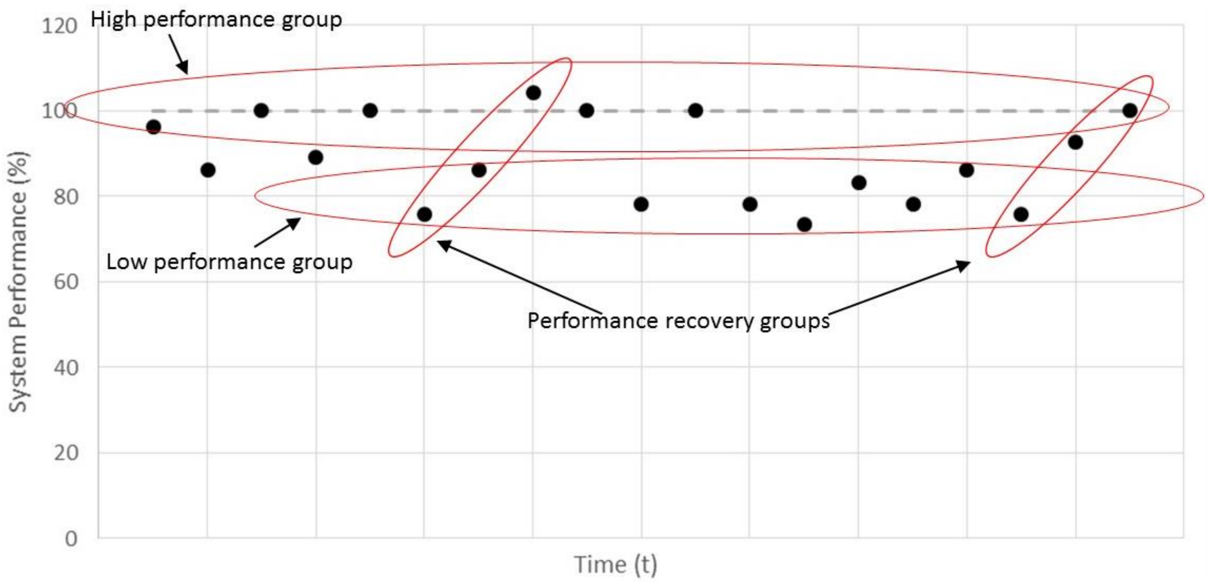


Figure 4.9: System performance measurements for driving car to work

Each measurement in Figure 4.9 has a functional signature. Each functional signature will provide insight to the functionality of the system for each measurement. Consider that a snapshot of one functional signature from the high performance group is displayed in Figure 4.10. This partial functional signature shows a portion of the functional activity that occurred on that drive to work. It is important to remember that this functional signature will be much longer than what is displayed, but it is not practical display the entire signature here. It can be seen that very specific functional outputs are recorded for each function, including the specific road you are on, the exact speed you are travelling, the road condition, if pedestrians are near, and so on. The particulars of each function will influence decisions that the driver will make on the way to work. It should also be noted that non-active functions during each occurrence of the model are not displayed here. This is optional and was done to remove clutter from the figure. If this functional signature provides insight into the functionality of one drive to work, then other drives to work can be compared to it. Do others from the high performance group exhibit similar/different functionality? The answer to this question will influence the way you may manage your drives to work.

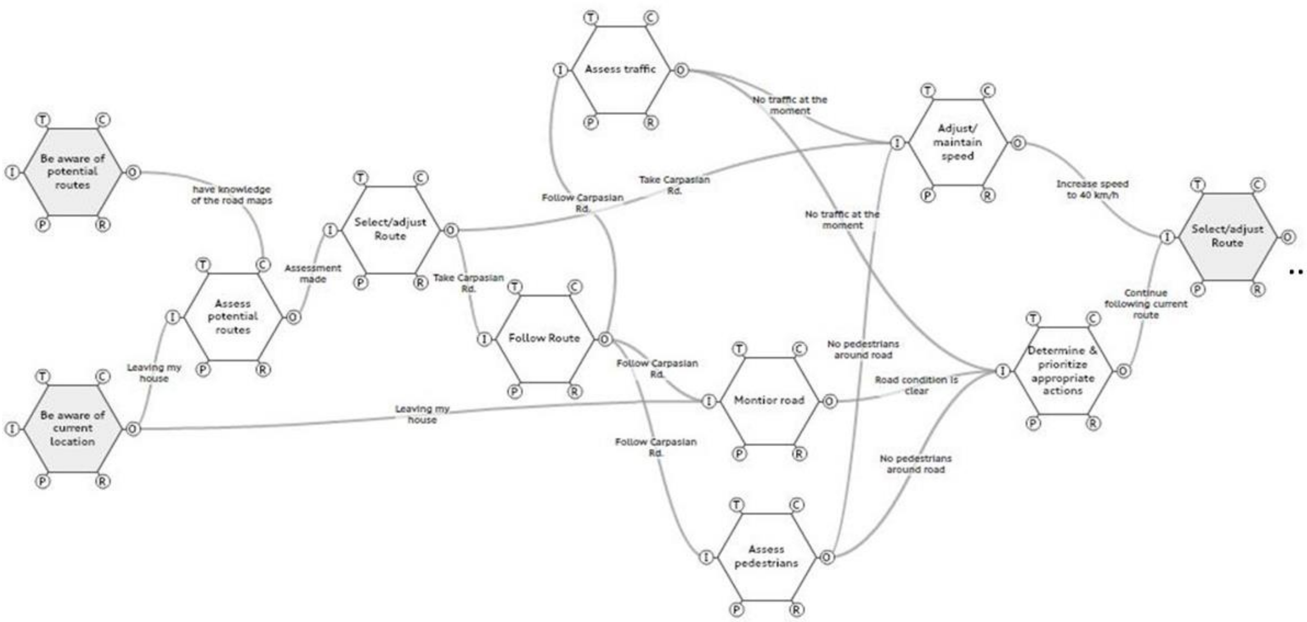


Figure 4.10: Snapshot of one functional signature

Figure 4.11 shows another snapshot of a functional signature. Suppose this signature is from the low performance group. This signature shows different particulars than Figure 4.10. Different roadways are used and an additional function (“Assess signage”) is active, which was not active for the snapshot shown in Figure 4.10. This signature can be compared to others in the low performance group and others in the high performance group. The understanding that is gained by examining these functional patterns and their relationships to high or low performance can help you manage your drives to work. Similarly, the functional signatures that occur during the time when system performance was recovering (see recovery groups - Figure 4.9) can provide insight to the mechanisms that promoted recovery. Understanding this recovery process may inform future management decisions that could promote quicker recovery.

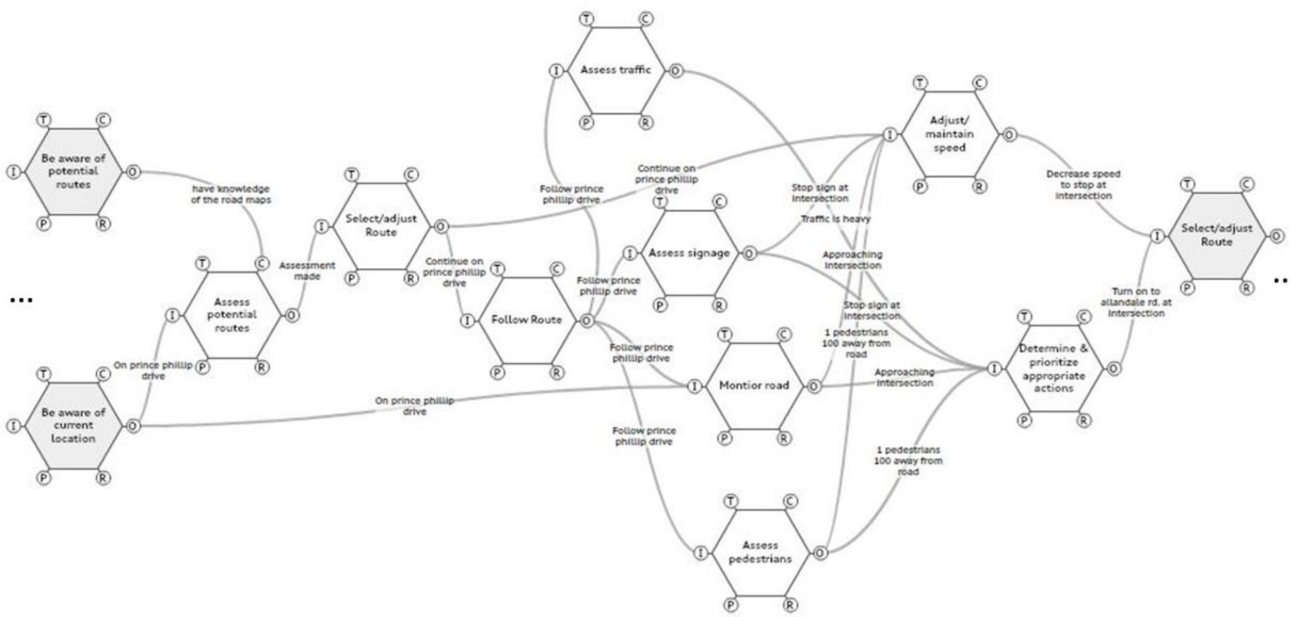


Figure 4.11: Snapshot of a second functional signature

While this example was chosen to provide a relatable example for readers of diverse backgrounds, the method can be applied in a similar manner for other applications. If the modelled operation is much more complex, the value of monitoring the system performance and tracking functionality would increase.

4.7. Conclusions

The methodology presented in this paper combines quantitative and qualitative techniques to provide a pathway for operators to evaluate, understand, and manage their operations using resilience. Using system performance measurement brings a quantitative element to the qualitative understanding of the functional assessment given by the FRAM, which allows for more informed evaluation of the qualitative information. Examining different performance levels allows for the identification of functional contributors for any level of performance. This information can then be used to support decision making for operators looking to promote or avoid certain levels of performance in their operation. Resilient elements such as robustness and rapidity can be understood by using this methodology as was seen in the examples in Section 3. This unique method can provide operators a means to understand their operation in a way that can support operational decision making based on quantitative and qualitative resilience concepts.

4.8. Acknowledgements

The financial support of the Lloyd's Register Foundation is acknowledged with gratitude. Lloyd's Register Foundation helps to protect life and property by supporting engineering-related education, public engagement and the application of research.

4.9. References

Ayyub, B. M. (2014). Systems resilience for multihazard environments: definition, metrics, and valuation for decision making. Risk Analysis: An Official Publication of the Society for Risk Analysis, 34(2), 340–355. https://doi.org/10.1111/risa.12093

Ayyub, B. M. (2015). Practical Resilience Metrics for Planning, Design, and Decision Making. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems., Part A: Civil Engineering, 1(3). https://doi.org/http://dx.doi.org/10.1061/AJRUA6.0000826

Béné, C., Headey, D., Haddad, L., & Grebmer, K. von. (2016). Is resilience a useful concept in the context of food security and nutrition programmes? Some conceptual and practical considerations. Food Security, 8(1), 123–138. https://doi.org/10.1007/s12571-015-0526-x

Borys, D., Else, D., & Leggett, S. (2009). The fifth age of safety: the adaptive age. Journal of Health & Safety Research & Practice, 1(1). Retrieved from http://chisholm.trainingvc.com.au/pluginfile.php/273772/course/section/28762/Journal%20article%20on%20adaptive%20age%20JHSRP_1-1_Borys_p19-27.pdf

Hollnagel, E. (2012). FRAM: The Functional Resonance Analysis Method. Ashgate Publishing Ltd.

Hollnagel, E. (2014). Safety-I and Safety-II: The Past and Future of Safety Management (1st ed.). Farnham, Surrey, UK England; Burlington, VT, USA: Ashgate Publishing Ltd.

Leveson, N. (2004). A New Accident Model for Engineering Safer Systems. Safety Science, 42(4), 237–270.

Manyena, S. B. (2006). The concept of resilience revisited. Disasters, 30(4), 434–450. https://doi.org/10.1111/j.0361-3666.2006.00331.x

Park, J., Seager, T. P., Rao, P. S. C., Convertino, M., & Linkov, I. (2013). Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems. Risk Analysis, 33(3), 356–367. https://doi.org/10.1111/j.1539-6924.2012.01885.x

Pelling, M. (2003). The Vulnerability of Cities: Natural Disasters and Social Resilience (1 edition). London ; Sterling, VA: Routledge.

Rothblum, A. M. (2000). Human Error and Marine Safety. Presented at the National Safety Council Congress and Expo, Orlando, USA.

Shappell, S., & Wiegmann, D. (2004). HFACS Analysis of Military and Civilian Aviation Accidents: A North American Comparison. Presented at the ISASI Seminar, Gold Coast, Austrailia.

UNISDR, (United Nations International Strategy for Disaster Risk Reduction). (2005). Hyogo Framework for 2005–2015: Building the Resilience of Nations and Communities to Disasters.

U.S. Department of Energy. (2009). Human Performance Improvement Handbook - Volume 1: Concepts and Principles (No. DOE-HDBK-1028-2009). Washington, D.C.

Vicente, K. (2004). The Human Factor: Revolutionizing the Way People Live with Technology. New York: Routledge.

5. VISUALIZING AND UNDERSTANDING THE OPERATIONAL DYNAMICS OF A SHIPPING OPERATION

5.1. Co-authorship statement

A version of this manuscript has been presented at the 2018 Society of Naval Architects and Marine Engineers (SNAME) Maritime Convention and has been accepted for publication in the SNAME transactions journal. The manuscript was written by authors, Doug Smith, Erik Veitch, Brian Veitch, Faisal Khan, and Rocky Taylor. Author Doug Smith led the writing of this manuscript, including the development of the methodology, the creation of the FRAM model, creation of the functional signatures, and the data analysis. Eric Veitch performed the ice management simulator experiment and shared that data. Erik Veitch also contributed to writing the Ice management experiment section of this paper and assisted with the data analysis. All authors revised, edited, discussed this work and made recommendations for improvements to its presentation.

5.2. Abstract

In this paper, a method is presented for visualizing and understanding the operational dynamics of a shipping operation. The method uses system performance measurement and functional signatures. System performance measurement allows assessors to understand the level of performance that is being achieved by the operation. The functional signatures then provide insight into the functional dynamics that occur for each level of performance. By combining system performance measurement with functional signatures, there is a

framework to help understand what levels of performance are being achieved and why certain levels of performance are being achieved. The insight gained from this approach can be helpful in managing shipping operations. Data from an ice management ship simulator is used to demonstrate this method and compare different operational approaches.

5.3. Introduction

In order for shipping operations to succeed, a complex set of dynamic operational conditions must be managed. The management of these conditions requires prior planning to ensure adequate resources are in place for operators, but the real-time dynamic conditions must also be managed, which require adjustments to be made to work processes by the ship's operators. The combined effect of managerial planning and operational actions determines whether or not the operation will succeed or fail. By considering the dynamic management structure of a shipping operation, it can be reasoned that the processes that produce both successes and failures are similar. The outcomes may be different, but processes behind them have many similarities.

Failures are often the focus of operational assessments where lessons are learned and management strategies are updated. In these failure based assessments, a large portion of the blame is typically placed on human error, roughly 70-90% in the maritime domain (Rothblum, 2000). This is reflective of the integral role humans play in operations. The hindsight bias that is present in retro-analytical assessments is not present for operators when they adjust to the operational conditions in real time. To manage an operation effectively, it should be understood what actions are producing good and bad outcomes, what conditions are present during these cases, and what conditions are promoting these operational responses. A better understanding of these questions can be obtained by also examining the successes of an operation with a focus on the processes that produce them. Traditionally, successes are not examined, or at least not examined at the same level of detail as failures. By modeling and tracking successful and unsuccessful outcomes together, there is an opportunity to better understand the operational dynamics of a shipping operation, which can be useful to inform ship management decisions. In order to effectively understand success and failure in the same model, the system should be modelled as comprehensively as possible, including the system's inter-relations. This is a systemic modelling approach. Systemic modelling is useful for modelling larger dynamic systems that have non-linear behaviors. In other words, the behavior of the system cannot be explained by reducing the system to its individual components and explaining the system as the sum of its parts. In this approach, it not appropriate to reduce systems to their individual components, so a certain level of complexity will be present to capture inter-relations between components. In order to understand this complexity, the concept of emergence is used (Hollnagel, Woods, & Leveson, 2006; Leveson, 2004). These non-linear behaviors will be difficult to predict and the behaviors may produce significantly different outcomes due to very small changes (or even no change) in the system conditions. In that sense, it is conceptualized that new understandings emerge, as the system is studied recursively over time. An assumption that the same initial conditions will produce the same outcome is not valid using this approach. As the outcomes and system behaviors are studied, new understandings will emerge for the system components and inter-relations.

This is an appropriate approach to apply to a ship operation, which is a complex socio-technical system (Morel & Chauvin, 2006).

We propose a methodology that allows understanding and visualization of a wide range of operational outcomes of a shipping operation. The method involves tracking the performance of the operation for every operational case (Ayyub, 2014). In order to do this, a suitable metric has to be used to track performance, which changes the concept of success and failure from binary to a continuous scale of performance ranging from low to high. Then to understand the processes that produce each outcome, we propose using the functional resonance analysis method (FRAM) (Hollnagel, 2012). The FRAM allows complex work processes and dynamic conditions to be visualized. By considering the variable performance of a shipping operation continuously, and then considering the work processes that produce them, there is an opportunity to learn from success as well as failure, better understand a complicated accident mechanism, such as human error, and ultimately more effectively manage ship operations. This method will be demonstrated here by using ice management simulator cases. This will help demonstrate how this method could be applied to a shipping operation.

5.4. Methodology

System performance measurement combined with FRAM can be used as a diagnostic tool for operational management and design. System performance measurement allows the performance of the operation to be monitored and provides insight to the level of performance that is being achieved by the operation. System performance measurement alone does not explain why certain levels of performance are being achieved. To help provide insight as to why a certain level of performance is being achieved, FRAM can be used. FRAM can help visualize the functional dynamics that occurred during a given operation, which resulted in the measured performance level of the operation. The functional dynamics are captured in a functional signature that is specific to each measurement. Once a number of performance measurements and functional signatures are collected, comparisons of the functional signatures that produce different levels of performance can be made. This could provide insight into good practices and poor practices. The managers can then try to promote the practices that result in high performance, and remove the practices that are linked to poor performance.

Consider the flow chart for this methodology shown in Figure 5.1. The first step is to define a metric that describes the performance of the system and build a FRAM model of the operation that will be considered. Then the system performance can be monitored and functional signatures can be tracked for the operation. Once a number of measurements and signatures are obtained, they can be compared individually and as groups. The signatures can be compared in terms of magnitude of outputs, functional paths taken, temporal distribution of functionality, and other quantities that may be of interest. Individually, the signatures can be examined to understand how the signatures of one measurement may be different from another. Additionally, the performance measurements can be grouped into bins and examined as groups, which could be useful in determining if there are common practices that are characteristic to a certain level of performance. After examining the functional signatures and the performance measurements, some insight related to system functionality and safety may emerge. If some insight is gained from the examination, it can be used to help manage the operation. If no insightful conclusions can be made from the examination, the system measurements and functional signatures can continue to be monitored. Insights may emerge with the inclusion of additional data. It is also possible that choosing a different bin size for the grouping assignment may allow for insight to emerge with different performance level groups.

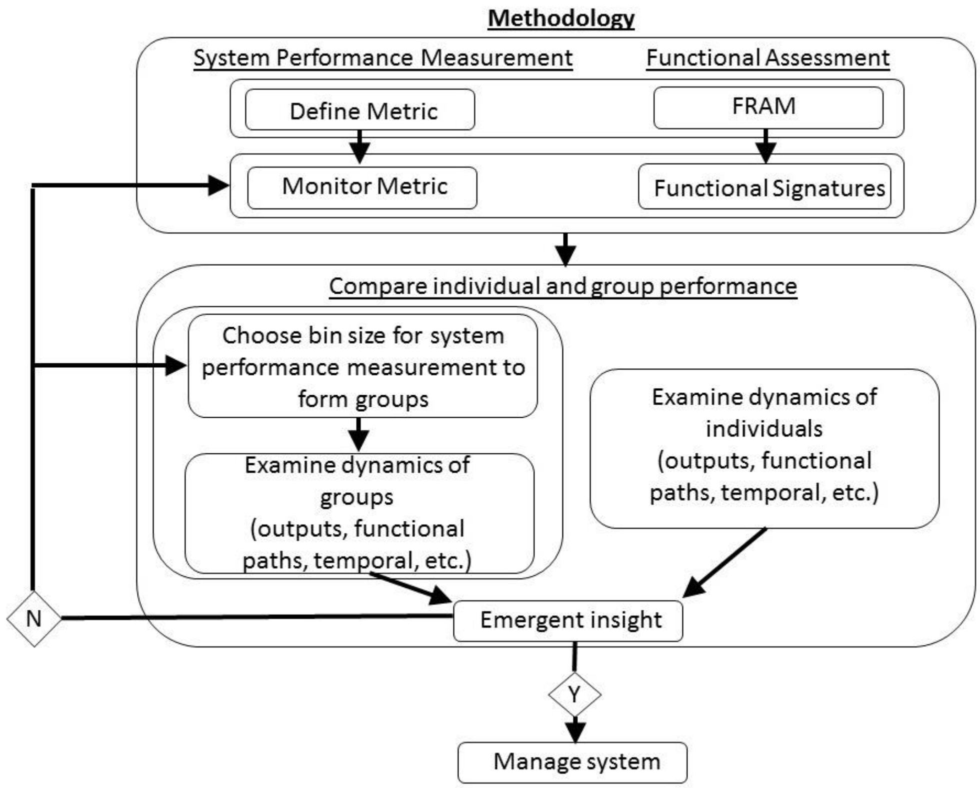


Figure 5.1: Flow chart of methodology

5.4.1. Functional Signatures

A FRAM model should describe the potential ways that the work can be carried out for an operation (Hollnagel, 2012). The FRAM model is a collection of nodes representing the functions or activities that make up the operation. The nodes (or functions) can be connected by different relationships: Inputs, Outputs, Time, Control, Preconditions, and Resources (Figure 5.2).

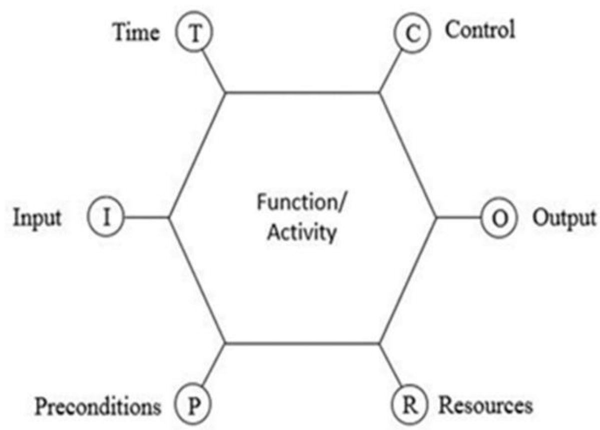


Figure 5.2: Node for FRAM model

The model does not describe the way the work actually happens. At any time (t), only a portion of the modelled functions may be active. The outputs that are produced by each function can also vary with time. In order to produce the functional signature for an operational case, the functional outputs and active functions are tracked over time. Figure 5.3 shows a functional signature at a time (t), where the active functions (shown in bold) and output variability is displayed (as an "output variation" label on the lines that extent from a function's output port).

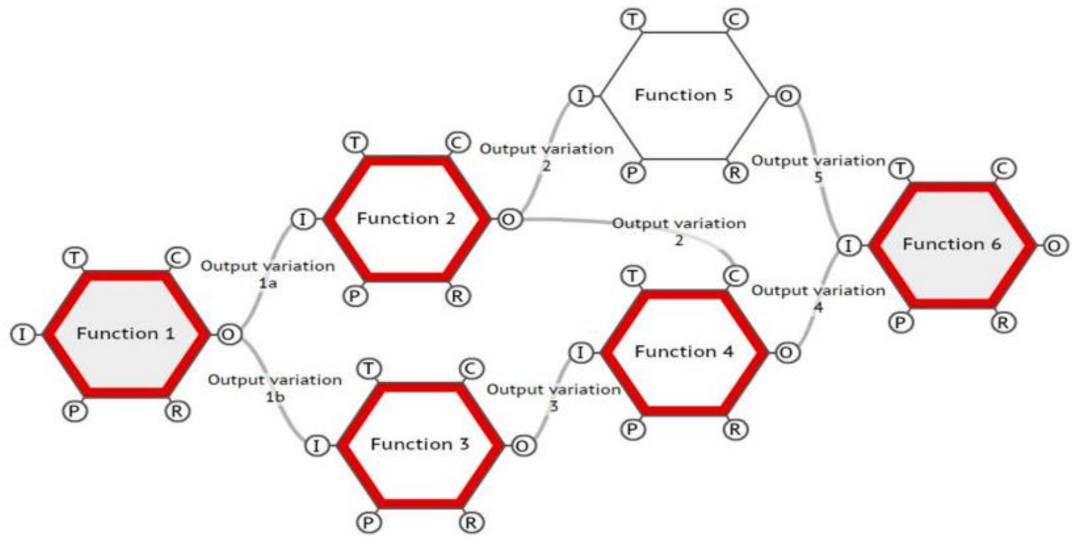


Figure 5.3: Functional Signature

5.5. Ice Management Simulator Experiment

An experiment was done using a ship simulator configured for an ice management operation. Thirty-three participants used the simulator to execute an operation that consisted of clearing pack ice from a lifeboat launch site at an offshore petroleum installation. Participants were also informed that their speed should not exceed 3 knots in the simulated ice conditions, as per the POLARIS ice navigation risk index in the Polar Code (IMO, 2017). The POLARIS system or similar support system has to be used by ships navigating in polar waters. This regulation is intended to prevent hull damage due to ice.

The simulator is powered by PhysX Rigidbody collision software (NVIDIA, 2017) and allows for full mission simulation tailored for specific vessels, geographic areas, wind, sea, ice, and current conditions. The simulator includes a (6½ ft by 6½ ft) platform that serves as bridge deck, mounted in the centre of a 360-degree panoramic projection screen (Figure 5.4).

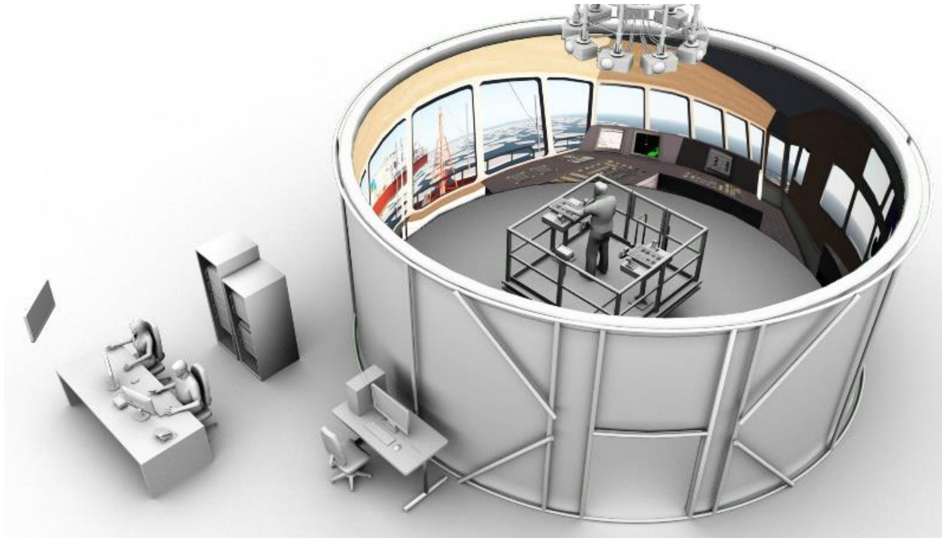


Figure 5.4: Sketch of the Ice Management Simulator setup

The Own-ship (the vessel in which the simulation takes place) is modelled as an Anchor Handling Tug Supply (AHTS) vessel. It has a length overall of 75m and is powered by twin 5369 kW diesel engines. For propulsion, it has two controllable pitch (CP) propellers and rudders, and forward and aft tunnel thrusters, each with 895 kW of power. The simulator has forward and after consoles from which to maneuver the vessel. To switch between consoles, the driver has to turn to the opposing console and transfer controls using “Transfer” toggle switches. Both consoles have identical basic controls: main propellers (port and starboard), steering, and tunnel thrusters (fore and aft).

Although the console provides all the fundamental controls for manual maneuvering, it was simplified for the experiment in that it did not include navigational aids like radar, GPS, or chart systems. While seakeeping and maneuvering characteristics were modelled closely to that which might be expected in reality, there were general limitations of similitude. In the face of such hardware and software limitations, the key to recording meaningful results stemmed from three controls: 1) each participant experienced the exact same experimental set-up, 2) no participant had encountered such a simulator before, and 3) each participant was given three “habituation” tasks, lasting almost an hour in total, which provided each participant with baseline experience with the simulator, including its minor limitations. These measures allowed the experimenters in the original study by Veitch et al. (2018) to focus on its main intention: to study the general strategies and techniques used in ice management.

An Instructor Station was used by the experimenters to control and monitor the experiment. A two-way radio provided the means of communication between the experimenters and the bridge officer on deck. Two experimenters were always within an arm’s reach of the radio; one provided the main instructions about starting and stopping the simulation; the other played the role of watch keeper, who provided information about distances to physical targets when prompted by the bridge officer during simulation.

An array of five computers collected data during the simulations. This included a time history of ice concentration within a specified zone, as well as position, speed, and heading. A video “Replay” file was also recorded during each simulation, which upon playback showed the entire simulation from start to finish. Figure 5.5 shows a screenshot example from such a Replay video.

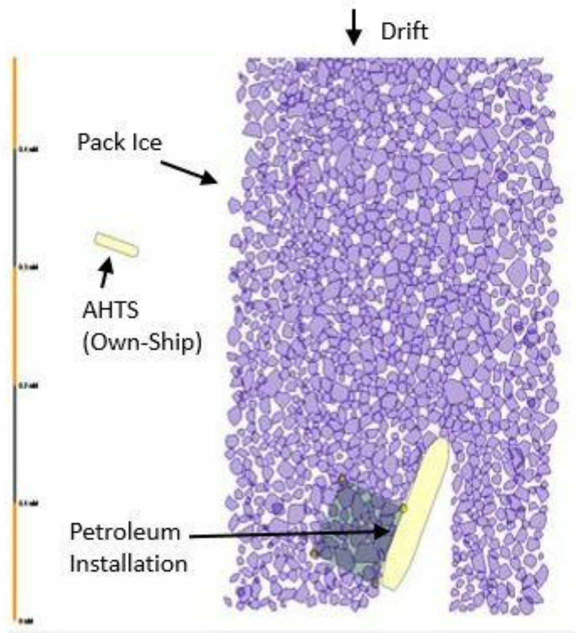


Figure 5.5: Snapshot of a replay file

5.6. Data Analysis

The data analysis of this experiment consisted of assessing the overall performance of each participant and determining the functional signatures for each participant, as per the methodology section.

5.6.1. System Performance Measurement

The metric used to define the performance of each participant is the percentage of time that the lifeboat launch zone was free of ice. Each participant performed ice management for 30 mins, so the best performing participants were deemed to have kept the area under the lifeboat launch zone ice free for the longest amount of time within the 30 minute simulation.

The lifeboat launch zone was defined as a circular area of radius 8 m located 8 m off the port quarter where the lifeboat davits are located. An image processing script was then used to determine if ice was present in the lifeboat launch zone. Figure 5.6 shows an overhead view of the circular area adjacent to the FPSO. The images were checked at a resolution of 30 s for the 30 minute simulation. The ice conditions in the circular area were assumed to be constant for each 30 s interval. After processing all 33 cases, the performance was determined for each participant.

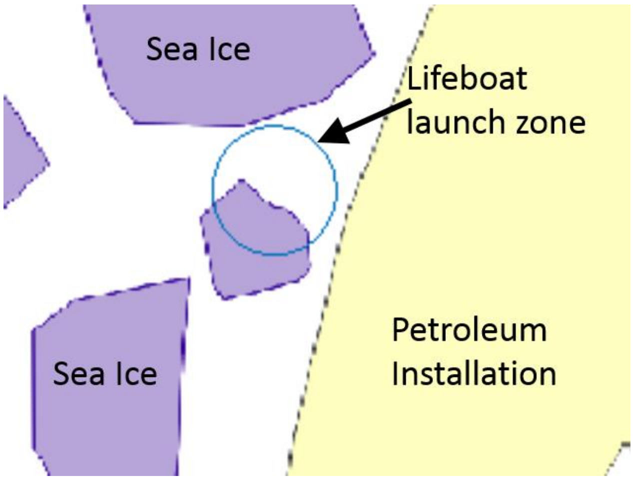


Figure 5.6: Lifeboat launch zone with ice piece inside

Figure 5.7 shows the range of performance that was observed over the 33 cases. Performance ranged from 63% to 0%, which corresponds to 18.9 and 0 minutes where the lifeboat launch zone is ice free during the 30 minute simulation. Each participant is identified by a label. Participant C79 performed the best in this experiment and C07, J42, S28, S41, and Z11 had the lowest performance

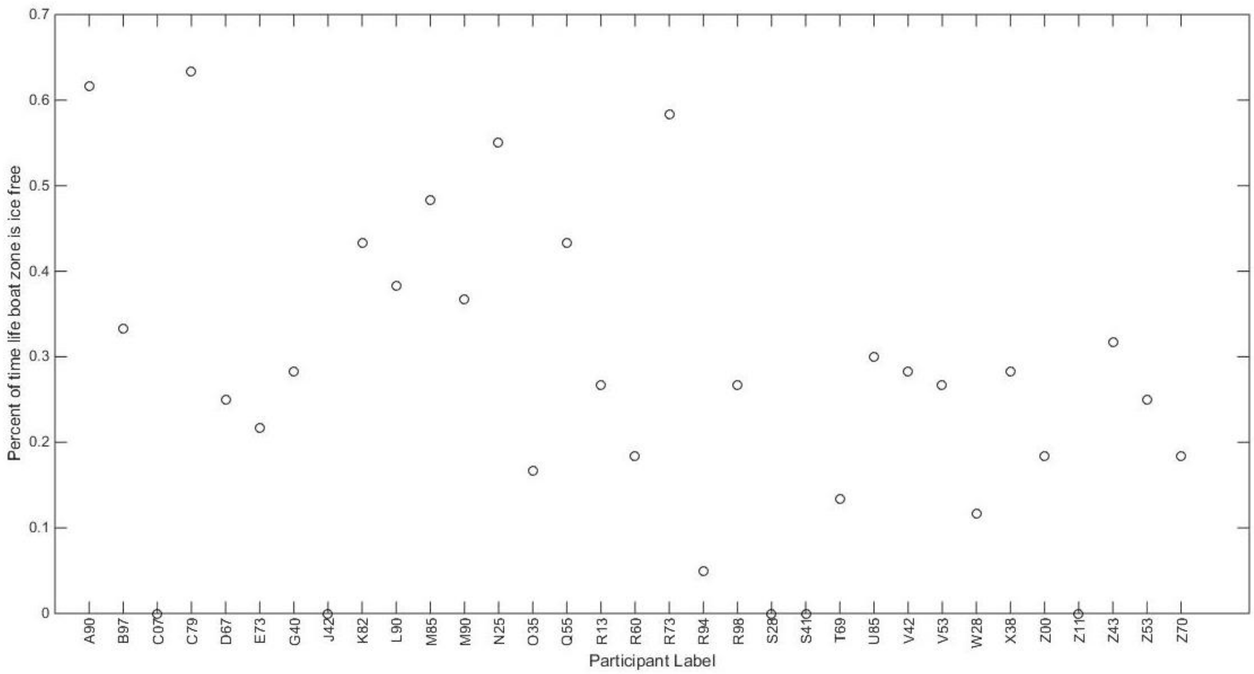


Figure 5.7: System performance measurements for experimental data

5.6.2. Functional Signature Analysis

A FRAM model was used to track the functional signatures for each participant. The FRAM model used can be seen in Figure 5.8. This model shows the potential functions that can be employed by the driver of the vessel in the experiment. The model is repetitive in the sense that it is a decision making model and each participant has to make many decisions over the course of the simulation. A ship navigator is constantly observing conditions, making assessments, and then deciding whether to maintain a course or make an adjustment (change course). Each function will have a dynamic output(s). The magnitude of the output(s) are displayed in the box that is located on the line that connects the function's output to a downstream function. Some functions will be more dynamic than others. For instance, the output of the function, "compute POLARIS risk index," does not change over the course of each participant's run. However, the awareness of this "static" output may influence the way each participant makes decisions (it is connected to a control node "make situational assessment" function). Conversely, changing course, monitoring vessel parameters, and observing the ice conditions happen many times over the scenario.

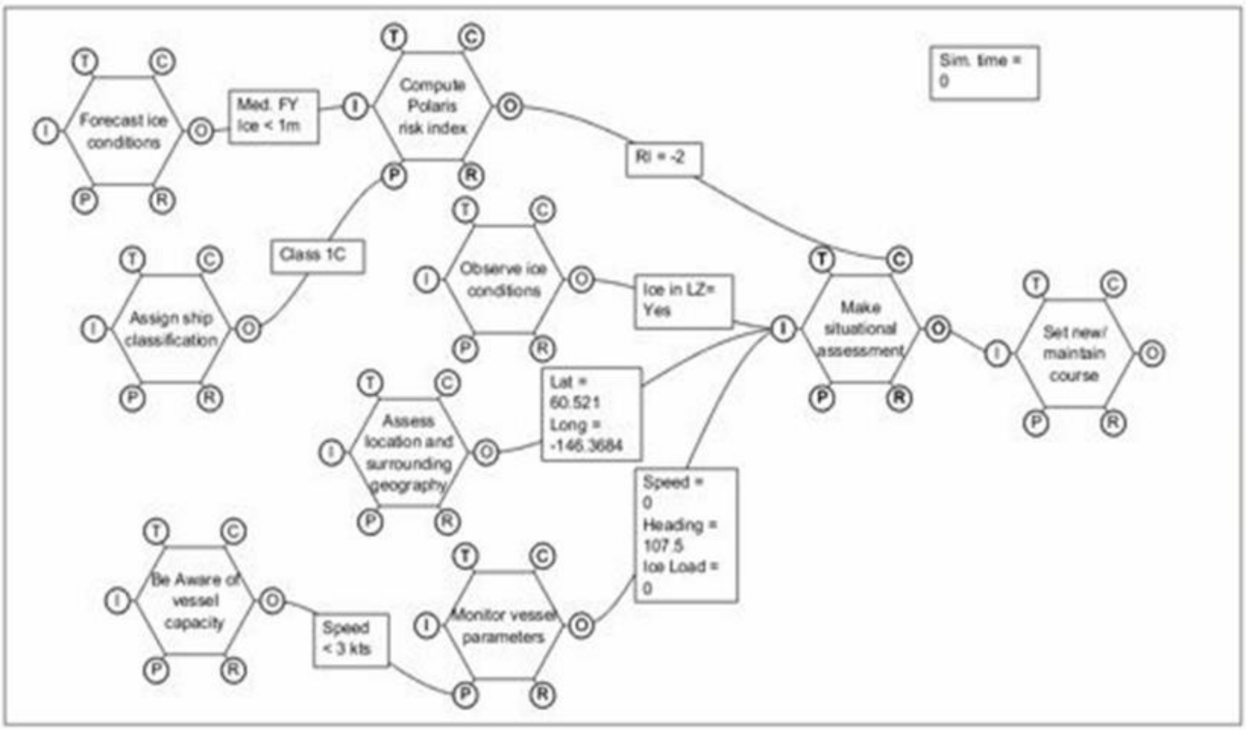


Figure 5.8: FRAM model for ice management simulator experiment

In order to determine when decisions and actions were made by the navigator, the functional signature was approximated. It is not known exactly when the participant was trying to make a course change (speed or heading), but it can be approximated by examining the peaks and troughs in the speed trace. A trough implies that a speed change was made to increase speed and a peak implies a speed change was made to decrease speed. See Figure 5.9 for an example of the approximated speed changes in the speed trace. The locations of the speed changes are circled. To filter out peaks due to signal noise, only peaks and troughs greater than 0.1 kts relative to the previous peak or trough were considered. Similarly, the vessel heading trace was used to approximate heading changes. See Figure 5.10 for an example of approximated heading changes in the heading trace. To filter out noise in the heading trace, only peaks or troughs greater than 5 degrees relative to the previous heading change were considered

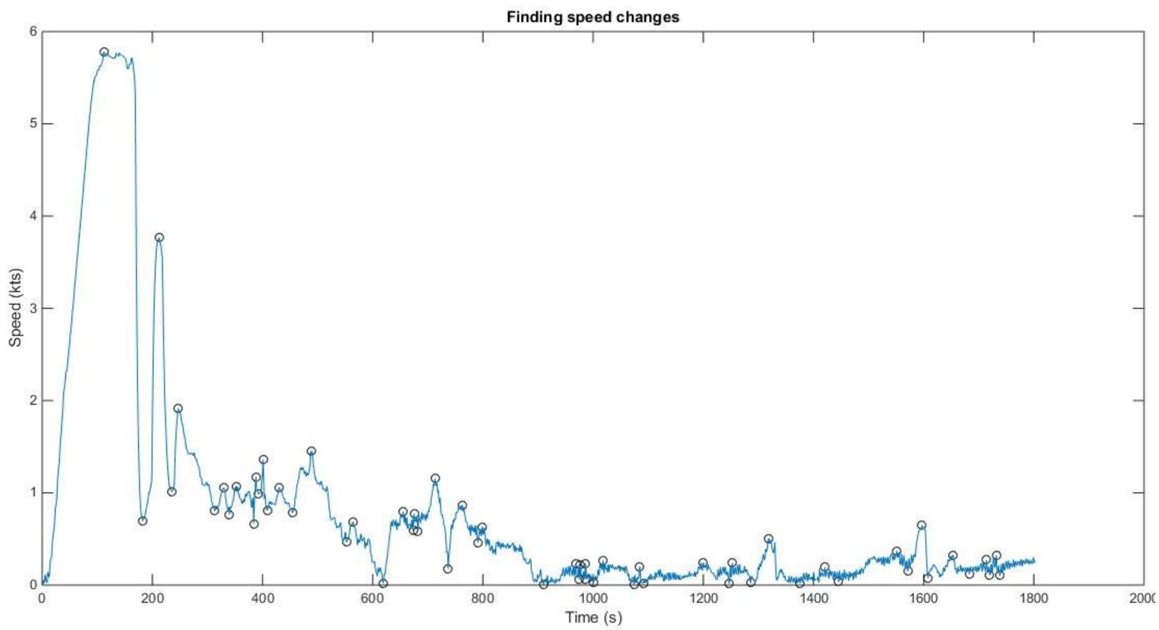


Figure 5.9: Finding peaks and troughs in a sample speed trace

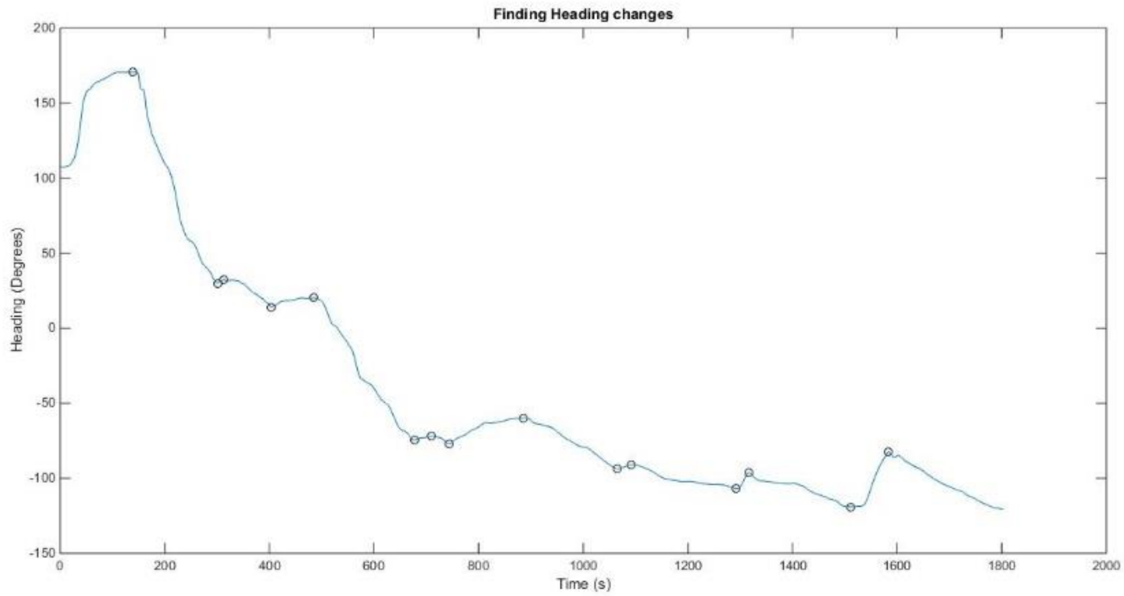


Figure 5.10: Finding peaks and troughs in a sample heading trace

The output for observing ice conditions was also approximated. It was assumed that the navigator checked the ice conditions in the lifeboat zone at least once every 30 s. This was the resolution of the data for the presence of ice in the lifeboat zone.

Times when the speed of 3 knots was exceeded and very high ice loads occurred were flagged. This can help understand when the highest ice loads were on the vessel, and particularly, the relationship between the highest ice loads and speeds above the regulatory maximum as imposed by the POLARIS system.

Based on these criteria, a case file was generated for each participant. The case file contained time stamped events, such as speed and heading changes, ice observations, speed limit violations, and very high ice loads.

This case file allows the functional signatures to be produced. As the simulated time elapses, the events in the case file can be displayed in a video format. This helps visualize the functional dynamics for each participant.

The best performing participant was C79. Snapshots from the functional signature from participant C79 can be seen in Figure 5.11 and Figure 5.12.

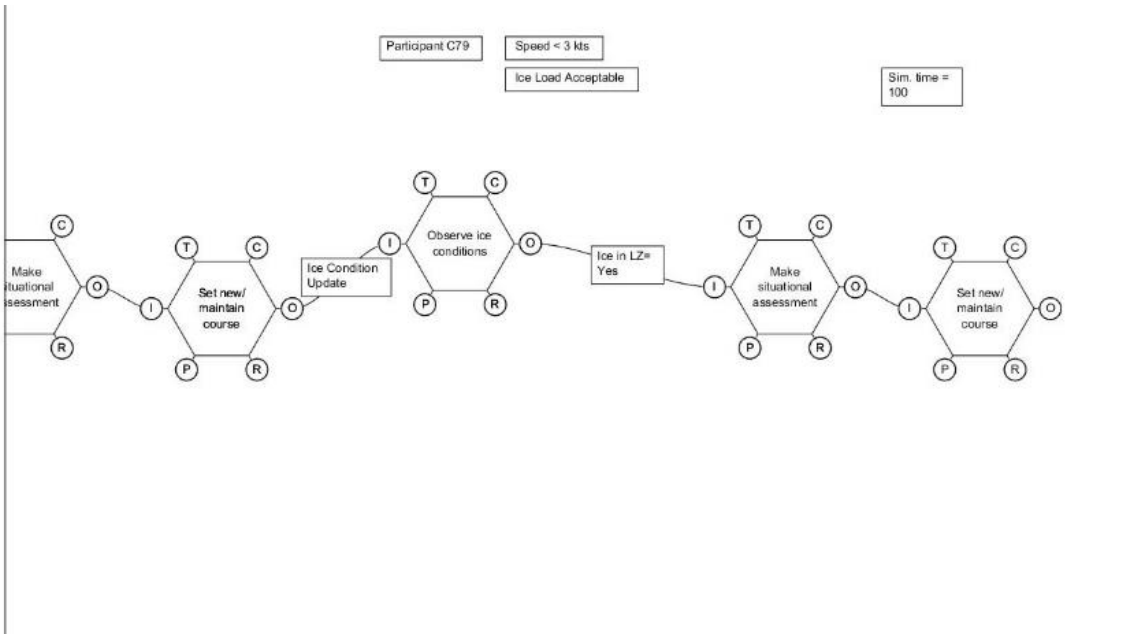


Figure 5.11: Snapshot of functional signature for participant C79 at 100 seconds

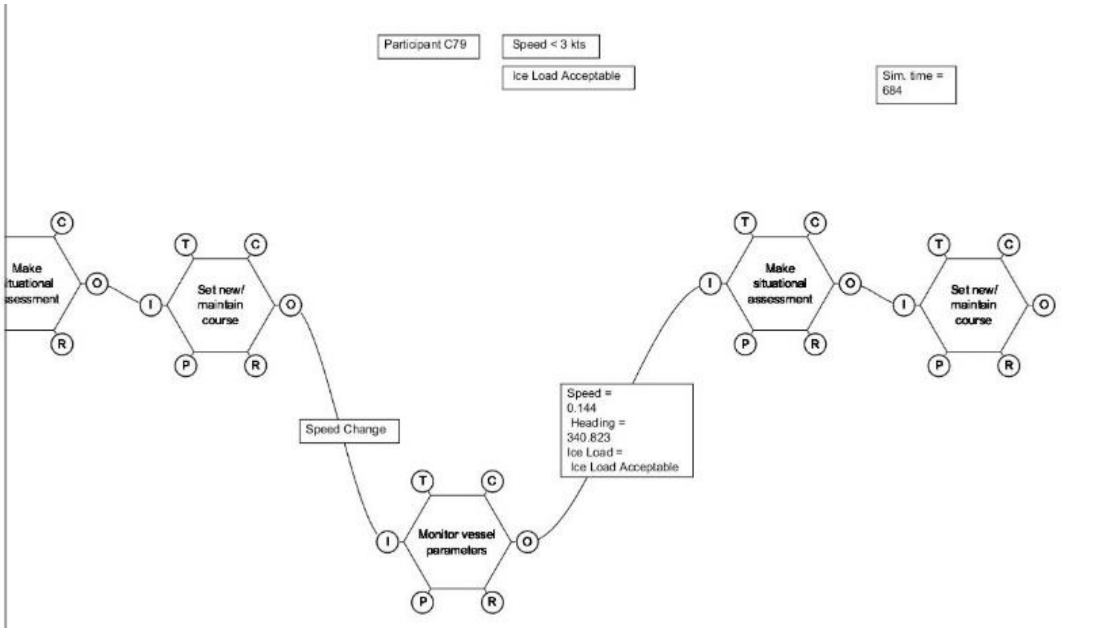


Figure 5.12: Snapshot of functional signature for participant C79 at 684 seconds

Also, snapshots of the functional signature from participant V42 can be seen in Figure 5.13 and Figure 5.14. The functional signature is different from C79, Figure 5.13 and Figure 5.14 show different functional paths and different outputs than for C79. This combination of functional activity and functional outputs happened to produce a lower level of performance.

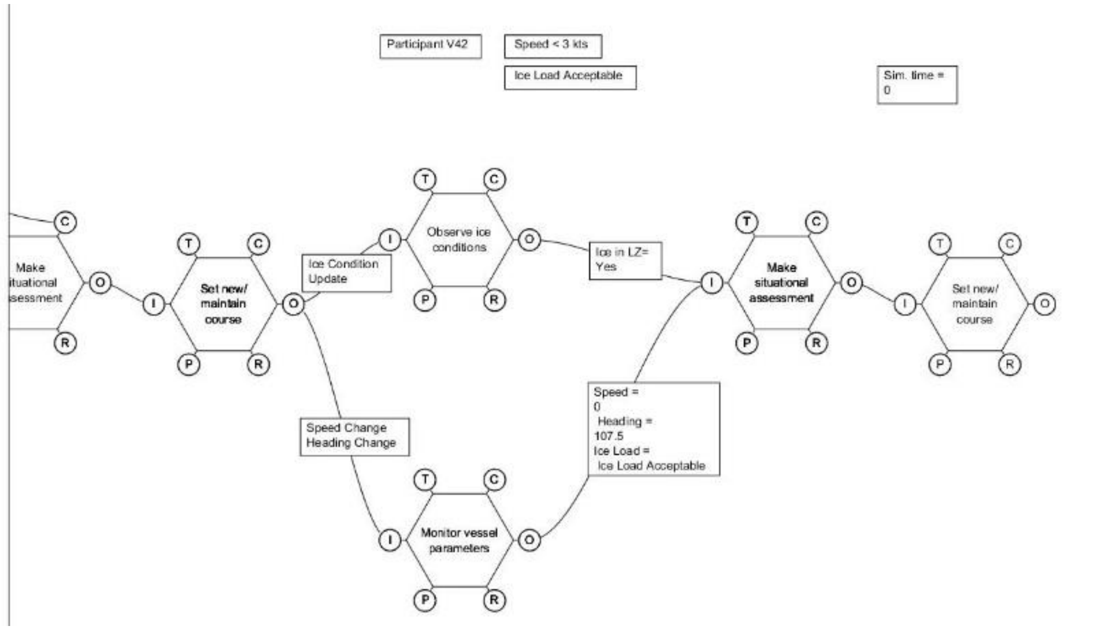


Figure 5.13: Snapshot of functional signature for V42 at 0 seconds

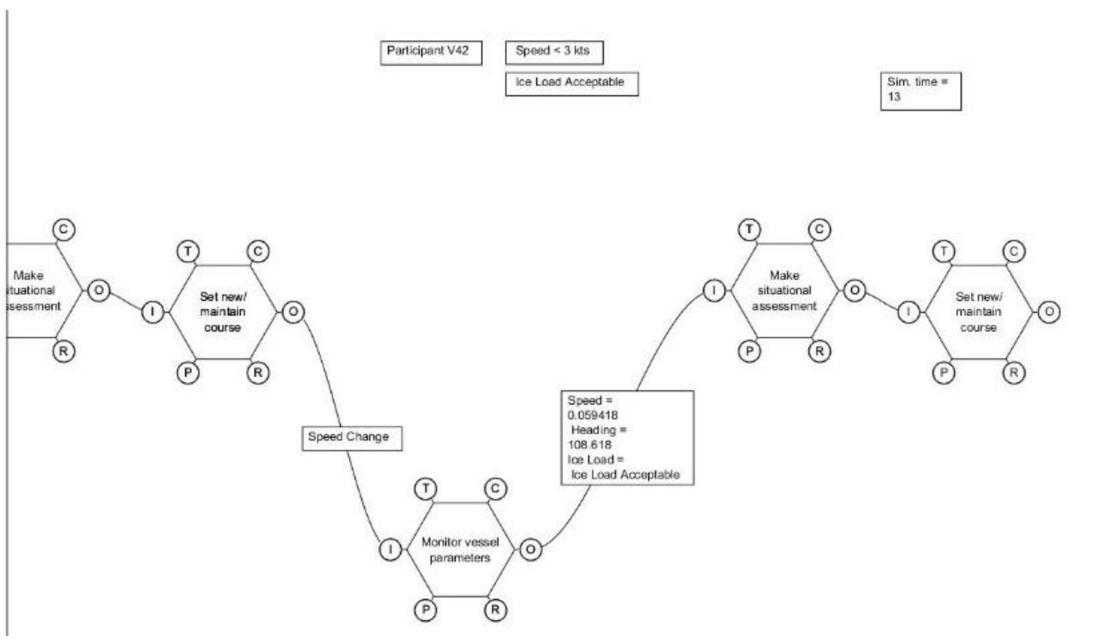


Figure 5.14: Snapshot of functional signature for V42 at 13 seconds

5.7. Comparison

After the functional signatures were approximated and the performance quantified for each participant, the functional signatures were compared. This can be a basis for understanding why one person performed better than another, and also for identifying practices that are common to high or low performance types. The functional signatures contain information pertaining to the function execution for each participant, including the outputs of tasks, the relationships between them, and the times at which the tasks occur. Once the operation has been tracked at this level of detail, there are many ways in which data can be examined. The comparison presented here is not exhaustive, in that there are other possible ways to analyze this data set. There are many ways functionality can be assessed to understand the execution and temporal aspects, and each way may allow different qualities to be understood. In this comparison, a moderate depth investigation of the functional signatures is made to demonstrate the method and obtain some understanding of effective and ineffective practices.

The first step is to bin the performance measurements from Figure 5.7 to "group" the data. The bins can be setup to the desired levels of granularity that the assessor wishes to investigate. In this assessment, the bins were chosen to be 0-25%, 25-50%, and 50-75% to represent poor performance, medium performance, and high performance, respectively, (see Figure 5.15). The groups are then examined using a boxplot. The boxplot bounds the 25th and 75th percentiles of the data, and contains a line in the box that represents the median. Whiskers extend from the box to the outer most data point that falls within +/- 2.7

times the standard deviation. Data points outside the limit are considered outliers and are denoted by a “+” symbol.

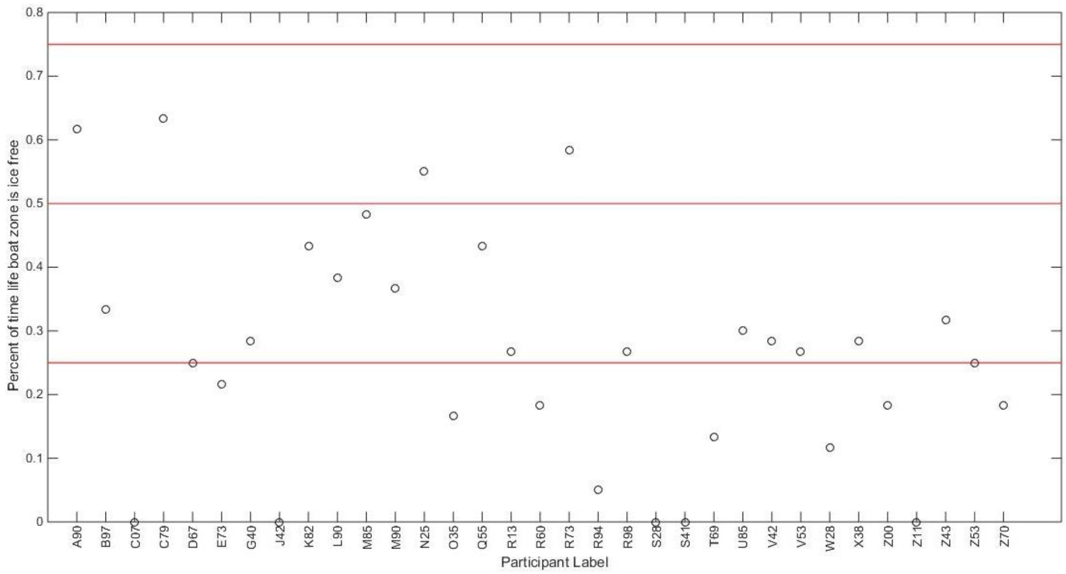


Figure 5.15: System performance measurements with bin size displayed (red line)

The groups were then examined to understand the functional activity of each group. This measure can provide insight into the level of functional activity that occurs in each group. Figure 5.16 shows the functional activity for the 3 groups in this assessment. For each group there is a wide variation in functional activity, with the 0.25-0.5 group having the least variability.

The number of specific active functions (number of speed changes, number of heading changes, and the number of ice observations in the lifeboat zone) can also be examined in a similar manner to determine which functions were the most active for each group.

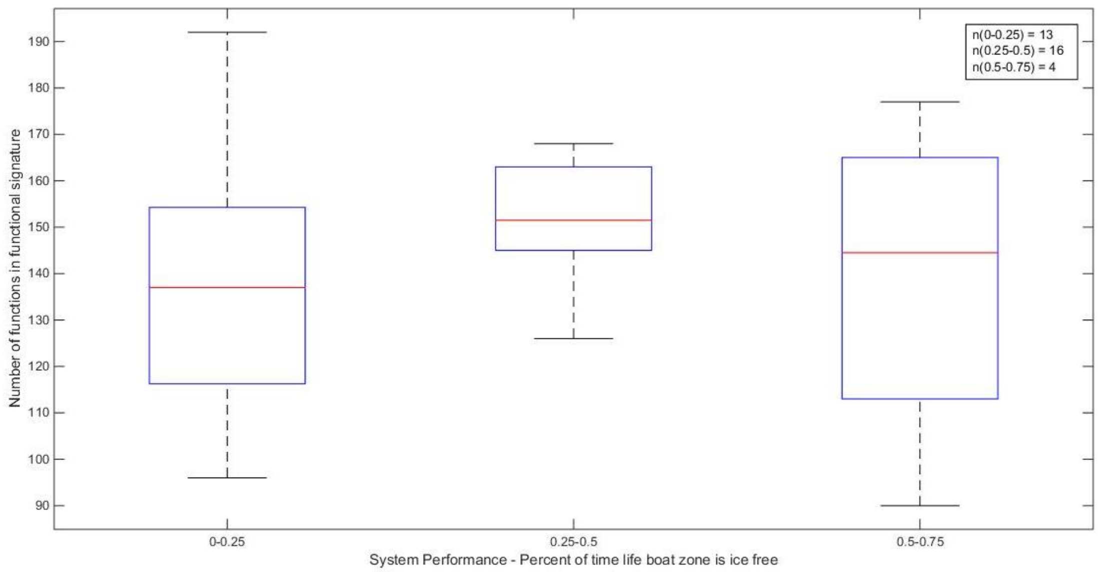


Figure 5.16: Functional activity of each group (n is number of participants in each group)

The temporal distribution of the functional signatures can be examined as well. Figure 5.17 shows the time distribution of active functions. It shows that the high performance group is more functionally active in the earlier part of the simulation than the other 2 groups. Similarly, the time distributions for each specific function can be examined this way.

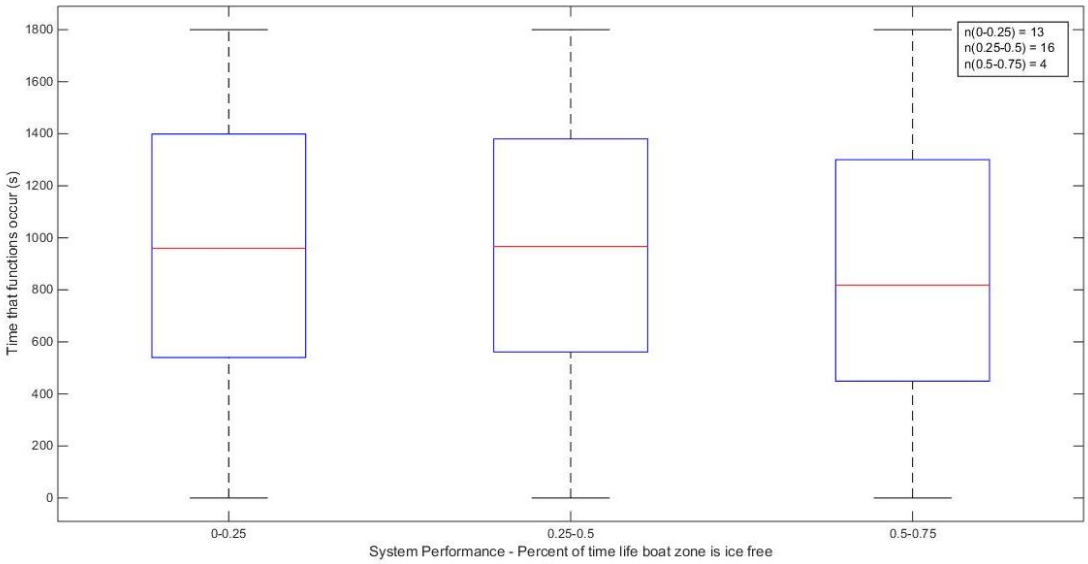


Figure 5.17: Time distribution of functional activity for each group

The variability for the functional outputs can also be monitored, which can be used to help understand the nature of the output variability for certain functions. For instance, the vessel speed is an output of the "monitor vessel parameters" function. This output is displayed in the functional signature every time the "monitor vessel parameters" function is active. Figure 5.18 shows the distribution of vessel speed for the participants' speed changes

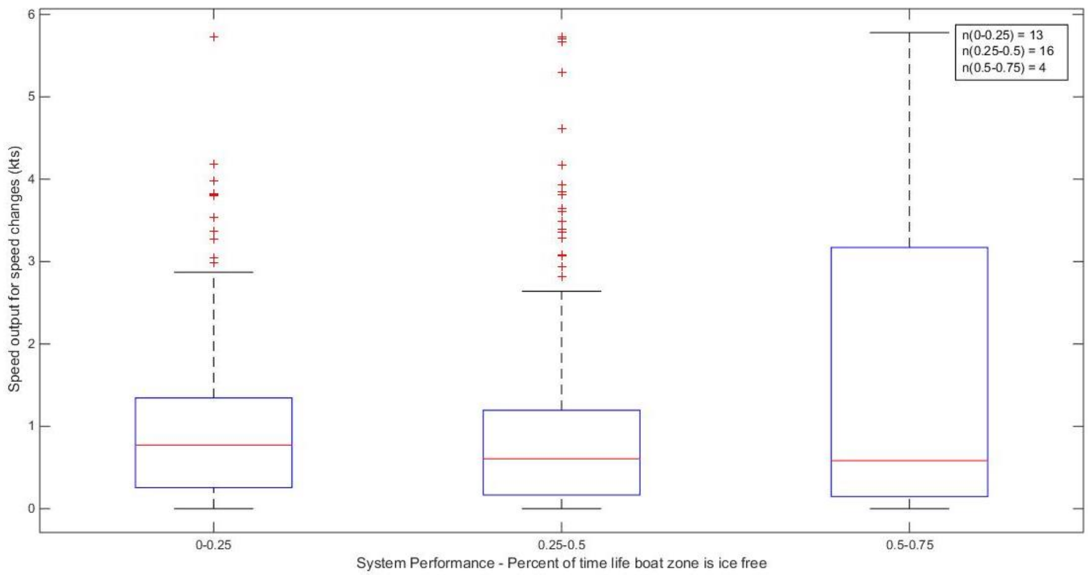


Figure 5.18: Speed output at speed changes for each group (kts)

The functional signatures promote the monitoring of many system parameters by way of functional outputs. This allows certain system parameters, such as regulations, to be examined. In many systems, regulations are created to improve safety, but rarely are the effects of the regulation checked to see if they are as intended. Also, the possibility that a regulation could have unintended effects on the system can be examined.

For example, the influence of the POLARIS ice navigation risk index can be examined. Two outputs that were tracked as outputs of the "monitor vessel parameters" function were the vessel speed and maximum local ice load on the hull. The number of speed violations and the speed at which high ice loads occur can be tracked. The ice loads computed by the simulator are not validated and therefore a qualitative scale of low, medium, high, and very high is used here to qualify ice load events. While the exact magnitude of the ice loads cannot be confirmed, this metric does give an indication of the points in the simulation where high levels of energy are being transferred to the ship's hull via ice. Figure 5.19 and Figure 5.20 show the number of speed violations that occurred for each participant and the speed at which very high ice loads occurred, respectively.

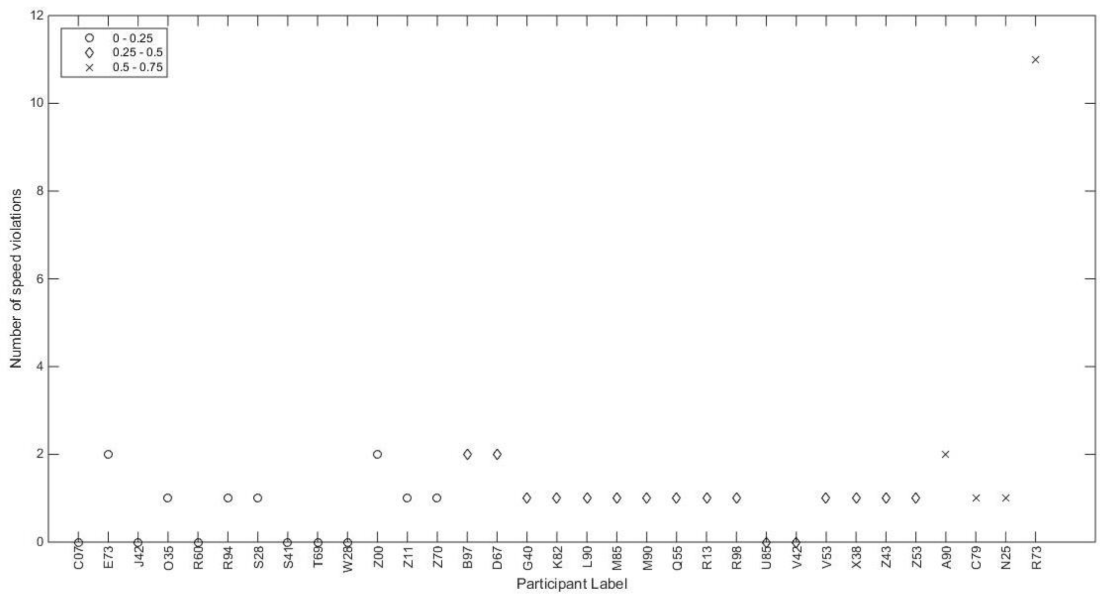


Figure 5.19: Number of speed violations per participant

From this examination, it can be seen there were speed violations recorded for most participants. The majority of participants had 0, 1, or 2 speed violations for the entire simulation, with the exception of "R73" who had 11. It is also of interest that "R73," who disregarded the speed limit the most, also performed in the top group with respect to clearing ice from the lifeboat zone. Figure 5.20 also shows that the majority of very high ice load events occurred at speeds below 3 knots.

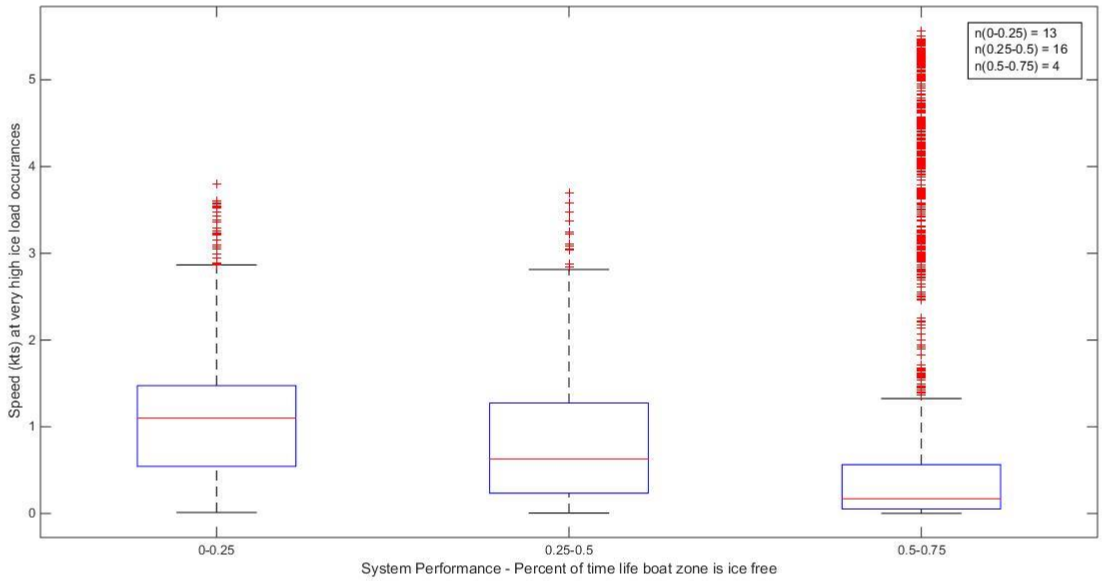


Figure 5.20: Vessel speed at very high ice loads

It is also important to consider each participant individually as well as by group. Consider the speed output of the high performance group (0.5-0.75 group) in Figure 5.18. The group data suggests that those participants transit the ice much faster than the other groups. However, by looking at the speed output over the entire speed trace for each participant, it can be seen that many of the high speed recordings were due to participant “R73.” The other 3 participants in the high performance group mainly operated at lower speeds. Figure 5.21 shows the speed distribution for the speed traces, which was logged every second, of each participant in the high performing group (0.5-0.75 group).

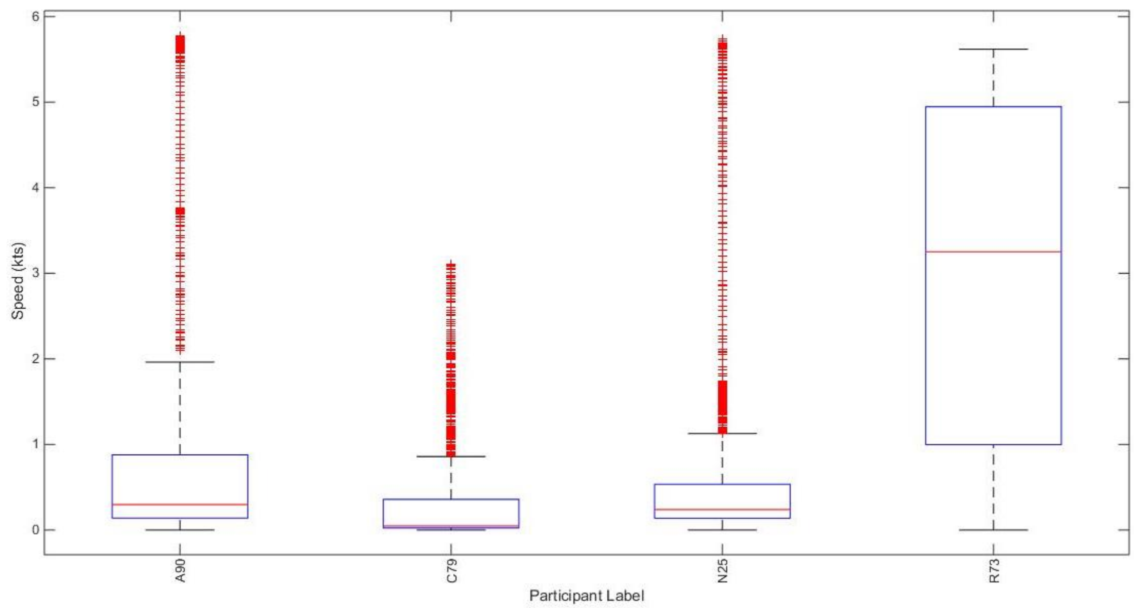


Figure 5.21: Speed distribution for each participant in the high performance group (0.5-0.75)

By further examining this group it can be seen that 3 participants, “A90”, “C79”, and “N25” had a similar approach to this operation, while “R79” had a different approach. “A90”, “C79”, and “N25” all approached the lifeboat zone from the south and moved to a position north of the lifeboat zone and held that position to block the south drifting ice from entering the lifeboat zone. “R79” moved quickly south and then north through the lifeboat zone, clearing away ice each time. Also, it was seen by examining the participants individually that “R73” was the quickest to clear ice from the lifeboat zone (see Figure 5.22). This was done by approaching the lifeboat zone from the north, which created an ice-free channel north of the lifeboat zone and pushed some of the ice downstream. By considering the variability in approaches, it may be reasonable to consider an approach that combines some of the best qualities of each individual of the group to create another approach that could be even better.

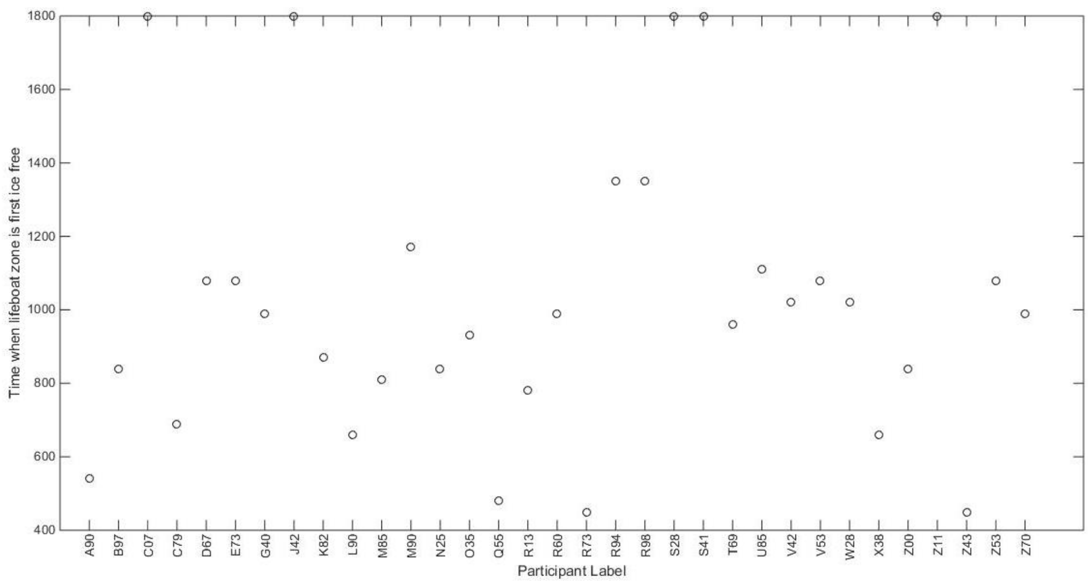


Figure 5.22: Time when lifeboat zone is first ice free

5.8. Conclusions

Operational practices influence performance of shipping operations. It is not always obvious which practices will produce certain outcomes because of the dynamic conditions in which ships operate. This paper presents a method to help visualize the way certain practices influence the performance of an operation. The method is demonstrated through the application of an ice management simulator experiment. A metric is used to measure the performance of each participant. This helps understand the level of performance that is being achieved, but does not help understand why certain levels of performance are being achieved. In order to provide more insight into why participants are achieving low or high performance, functional signatures are used to monitor the system functionality. This paper demonstrates some of the ways a comparison may be made to examine the performance data. In this example, enough insight was obtained to understand some qualities of high and low performance and suggest an approach for improving future performance. These are valuable insights for system management.

Some people may have reservations about using data from ship simulators to manage real operations, which opens up a different discussion. However, the main focus of this paper is to present and demonstrate a novel method for managing ship operations. This method has been demonstrated using data from a ship simulator, but the method could be applied in the same manner to actual ship data should an operator wish to do so.

The PMPM method is born of the need to make improvements to safety management. Some discussion of how safety management might be approached when using this method is warranted to more clearly link the method to the original safety management objectives of this thesis. The PMPM method is an investigative tool that allows users to closely monitor changes in functionality and compare them in terms of the influence on system performance. The method provides insight into the system but does not explicitly suggest how safety management decisions should be made. A question may be posed, as to how we know that we are making the best decision? In most cases, the best decision would be the decision that results in the best outcomes for the operation. However, safety management decisions need to be made prior to the outcomes being known so it is difficult to exercise that criterion for decision making at the decision time. This gap between decisions and future outcomes bring about inherent uncertainties that are usually dealt with by making some leap of faith that is bridged by your system resilience and robustness. If outcomes cannot be guaranteed for safety management decisions, then another criterion for decisions might be, to make the most informed decisions as possible. By becoming more informed, a better understanding of the system will be the basis of the decision, which can serve to reduce the risk to unfortunate outcomes occurring as one traverses the gap between decision and outcome. The PMPM claims to improve the quality (and quantity) of information that is used to inform safety management decisions, which by the second criterion can translate into improvements to safety management.

5.9. Acknowledgements

The authors acknowledge with gratitude the financial support of the NSERC-Husky Energy IRC in Safety at Sea, and of the Lloyd's Register Foundation.

5.10. References

Ayyub, B. M. (2014). Systems resilience for multihazard environments: definition, metrics, and valuation for decision making. *Risk Analysis: An Official Publication of the Society for Risk Analysis*, *34*(2), 340–355. https://doi.org/10.1111/risa.12093

Hollnagel, E. (2012). *FRAM: The Functional Resonance Analysis Method*. Ashgate Publishing Ltd.

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience Engineering: Concepts and Precepts*. Hampshire, UK: Ashgate Publishing Ltd.

IMO. (2017). International Code for Ships Operating in Polar Waters (Polar Code).

Leveson, N. (2004). A New Accident Model for Engineering Safer Systems. *Safety Science*, *42*(4), 237–270.

Morel, G., & Chauvin, C. (2006). A socio-technical approach of risk management applied to collisions involving fishing vessels. *Safety Science*, *44*(7), 599–619. https://doi.org/10.1016/j.ssci.2006.01.002

NVIDIA Corp. (2017). Rigid Body Collision — NVIDIA PhysX SDK 3.4.0 Documentation. Retrieved August 10, 2018, from https://docs.nvidia.com/gameworks/content/gameworkslibrary/physx/guide/Manual/RigidBodyCollision.html

Rothblum, A. M. (2000). Human Error and Marine Safety. Presented at the National Safety Council Congress and Expo, Orlando, USA.

Veitch, E., Molyneux, D., Smith, J., & Veitch, B. (2018). Investigating the influence of bridge officer experience on ice management effectiveness using a marine simulator experiment. *Journal of Offshore Mechanics and Arctic Engineering*. https://doi.org/10.1115/1.4041761

6. CONCLUSIONS & RECOMMENDATIONS

6.1. Conclusions

Safety is paramount for Arctic shipping operations. Many of the risks associated with ships in the Arctic are unaffordable, making learning from mistakes as the primary focus inappropriate. In this context, a more proactive approach to safety is needed. This research focuses on using the system and safety II paradigms for developing a methodology that can be used to inform safety management. These paradigms are the foundations for the performance measurement and process mapping/monitoring (PMPM) method that is presented in this work. The PMPM method marries qualitative techniques: the FRAM and functional signatures, with a quantitative technique: system performance measurement. The combination of quantitative and qualitative understandings that can be gained from the PMPM method provides a framework that allows for diagnostic safety management of complex socio-technical operations. The use of the FRAM provides guidance to monitor and assess the inner workings of operations. The incorporation of system performance measurement brings a quantifiable element to the FRAM that can aid assessors and decision makers in comparing different scenarios. System performance measurement allows the overall performance of an operation to be quantified. The concept of functional signatures is an extension of the current FRAM that can be used as a visual tool to bring more understanding regarding the inner workings of operations, in particular in the functional dynamics. This method is appropriate for safety management in Arctic shipping, but may be useful for other domains, especially if the operation is dynamic and socio-technical.

When this method has been demonstrated throughout this thesis, ship navigation has been area of application. When building the FRAM model for ship navigation, ship captains were used as the basis to inform the modelling. This provides information regarding the functions that ship captains perform when navigating ships. Also, the information regarding variability collected from the captains is relevant to the ways they perform their tasks, and how they might respond to certain operational conditions. The use of data from a ship simulator performing an ice management operation was also used to demonstrate the complete method presented in this thesis. From this data set it is demonstrated how to rank the overall performance for different system measurements, create their functional signatures, and possible ways to compare quantities of the functional signatures. These demonstrations can be used as starting points for future assessments in ship navigation or as a basis to transfer the method to other domains.

6.2. Recommendations and Future Work

This thesis shows the theoretical framework for the PMPM method and demonstrates it using a few applications to Arctic shipping. From the few limited applications of this method, it seems to be a reasonable approach. It is recommended that this method continue to be used to investigate safety. By using this method more, there is an opportunity to learn about specific applications and possibly about the overall utility of the method, and any limits to appropriate applications that may exist. There is an opportunity to be able to understand the signatures of certain intangible qualities of safety, such as safety culture. This can be explored by using the method to see if certain characteristics of safety culture may emerge in a FRAM analysis, and by using system performance measurement there is a way to use quantification to measure the overall effect of those characteristics.

Further quantification of this method may be desirable in the future. There are two possible ways that additional quantification may be used: 1) Develop a system for quantification of each functional output in a FRAM model and 2) have multi-variable system performance measurements. Quantification of individual functional inputs would allow for intermediate monitoring throughout the operation and provide a better opportunity to locate safety concerns within the system. This level of quantification is already achievable for functions that have outputs that are easily quantified. The challenge for the future work is to create a reasonable system for quantifying the outputs of functions that are difficult to measure on quantifiable scales. Multi-variable system performance measurements may allow for more complete representation of functionality through system measurements. The current approach uses a single measurement to quantify performance, which is then used to make judgments about its influence on functionality, which can inform safety management decisions. The guidance is to select a single measurement that represents the main objective of the operation. However, there could be cases where improving on that measurement may be at odds with improving on safety. A multi-variable approach that can synthesize variable measurements might be a useful way to overcome this.

It may be useful to further develop techniques for visualizing functional signatures. More detailed techniques that allow functional dynamics to be monitored with higher precision may be an advantage. The current technique for functional signatures shows snapshots of the functionality in the operation over time. At any given time, the functional signature is showing the functionality over a time range, even if that range can be reduced to a fairly short interval. It may be useful in the future to add a highlighted "spot" on the functional signature that shows the instantaneous location of functional activity on the signature. This technique could also be useful for visualizing functional activity in parallel paths of the functional signature, especially if the functional activity of those paths move at different rates. This improvement could be useful for visualizing complicated, time dependent operations.

7. Appendix A

ICEHR – Application for Ethics Review (Secondary Use of Data)

Project Info.

File No: 20181986

Project Title: Using FRAM to assess the performance of ice management for offshore installations using simulated environments.

Principal Investigator: Mr. Doug Smith (Faculty of Engineering and Applied Science)

Start Date: 2018/03/09

End Date:

Keywords: Engineering,Oil and Gas

Related Awards:

Award File No	Principal Investigator	Project Title	Funding Snapshot	Notes
20171763	Brian Veitch	Safety management of arctic shipping	RDC Program: ArcticTECH Program	N/A

			Type: Contract-Agreement Account#: 212013 41000 2000 Requested: CAD 249,061.00 Awarded: CAD 249,061.00 PROJECT TOTALS: Requested: CAD 249,061.00 Awarded : CAD 249,061.00	

Project Team Info.

Principal Investigator

Prefix: Mr.

Last Name: Smith

First Name: Doug

Affiliation: Faculty of Engineering and Applied Science

Rank: Doctoral Student

Email: r35drs@mun.ca

Phone1: 709-427-4275

Phone2:

Fax: 709-864-4042

Primary Address:

Institution: MUN (STJ)

Country: Canada

Comments:

Other Project Team Members

Prefix	Last Name	First Name	Affiliation	Role In Project	Email
Mr.	Veitch	Erik	Faculty of Engineering and Applied Science\Department of Ocean and Naval Architectural Engineering	Co-Investigator	erik.veitch@mun.ca
Dr.	Veitch	Brian	Faculty of Engineering and Applied Science\Department of Ocean and Naval Architectural Engineering	Supervisor	bveitch@mun.ca

Common Questions

1. Degree Program

#	Question	Answer
1.1	Please indicate the project program related to the application.	Doctoral Dissertation
1.2	If OTHER, please specify.	N/A

2. Purpose of Study and Research Questions

#	Question	Answer
2.1	Explain the purpose, objectives, and hypotheses of the project in non-technical, plain language. (Maximum 500 words)	Prior to this study, we have built a model using the functional resonance analysis method (FRAM) of the way shipping operations function. This modeling technique requires that the tasks used to carry out the operation be represented as functional nodes and the collection of nodes (tasks) should have connections that describe the nature of the inter-dependencies between the tasks that are being modeled. To verify this model and demonstrate it's utility, it should be used by collecting data and comparing the modeled results to the practical results. The ideal data source for this is to collect data from a shipping operation. This will give you a sense of how well your model reflects realities of a shipping operation. However, we have had trouble recruiting participants from actually shipping operations, which we believe is due to time commitments and liability concerns of what they will be asked. Another opportunity to collect data to demonstrate this modelling technique is using ship simulator data. An experiment using an ice management simulator has been conducted by Erik Veitch et al. This experiment collects

		data from participants to drive a simulated vessel to clear ice away from a life boat launch zone for an offshore petroleum installation. This data can be used to be analyzed by the FRAM. The FRAM will assess the tasks that were completed by each participant in the simulator and connect their task performance to their ability to clear ice in the simulated environment.

3. Data Characteristics and Background

#	Question	Answer
3.1	Select the relevant data type(s):	Data anonymized AFTER collection
3.2	Provide a summary description of the source data to be used in the proposed project. Indicate the nature / type of data, how and why it was originally collected and by whom, and how you will obtain access to the dataset(s).	The source data is "Operating window for moored floating structures in harsh environments." PI: Erik Veitch and File No: 20170540. The data was collected by Erik Veitch under the conditions of the above mentioned project. I will obtain the post-processed anonymized data.
3.3	Describe the size of the dataset(s) and/or number of original participants in the data collection.	There are 72 participants in this experiment. Each file contains 30 mins worth of data which was recorded from the simulator, including vessel speed, heading, ice load and ice concentration.
3.4	Explain any criteria that will be used to identify / select relevant data such as specific participant attributes, periods of time, or geographical location.	This assessment will not consider any particular attributes of participants. Only the outputs from the ice management simulator.
3.5	Was any of the source data originally collected for research purposes?	Yes
3.6	If YES, specify the REB that approved the original data collection. If the original REB was ICEHR, provide the	The source data is "Operating window for moored floating structures in harsh

	ICEHR file number. If the original data collection did NOT have REB approval, explain why not.	environments." PI: Erik Veitch and File No: 20170540.
3.7	If the source data was NOT originally collected for research purposes, indicate the purpose(s) of the original data collection.	
3.8	If OTHER, please specify.	N/A
3.9	Was the data collected with consent from participants?	Yes
3.10	If YES, describe the elements of consent regarding data sharing and future use that participants agreed to. If available, upload a BLANK or REDACTED copy of the consent form used for the original data collection in the Attachments tab.	See informed consent form from: "Operating window for moored floating structures in harsh environments." PI: Erik Veitch and File No: 20170540.

4. Access to Data, Privacy, and Confidentiality

#	Question	Answer
4.1	Identify the source(s) of the data (e.g. government agency / department, other public body, or private company / individual)	The source data is from "Operating window for moored floating structures in harsh environments." PI: Erik Veitch and File No: 20170540.
4.2	Is the data available in the public domain? (See description above)	No
4.3	Identify the data custodian / holder for each data source identified in 4.1 and upload a copy of the correspondence communicating approval and/or granting access to the data in the Attachments tab.	Erik Veitch. All communication regarding this secondary use of this data was verbal.
4.4	Describe how data will be securely obtained / transferred and stored for use in this project.	The data will be transferred as anonymized excel files that contains data on the simulated ship and ice conditions in each simulation.

4.5	Are there specific retention and/or destruction parameters placed on the data by the data holder / custodian? If YES, discuss.	No
4.6	As per Memorial University's policy on Integrity in Scholarly Research, all primary data resulting from scholarly activity must be retained for a MINIMUM of 5 years. Please provide details regarding your anticipated plans for retention and/or disposal of the data.	After 5 years the data will be disposed of as per the the conditions of file No: 20170540.
4.7	Will data be shared with or accessed by anyone other than the principal investigator?	Yes
4.8	If YES, describe how data will be shared and in what format.	The data files will not be shared, but the results from the FRAM analysis will be presented in a Journal Publication.
4.9	Will data from this study be contributed to a larger study?	No
4.10	If YES, identify any other institutions and/or external team members involved in the larger study.	N/A

5. Data Linkage

#	Question	Answer
5.1	Will the proposed project require data linkage?	No
5.2	If YES, describe how confidentiality of the data will be protected, who will perform the data linkage, and how the merged files will be safeguarded?	N/A
5.3	If YES, is this linkage likely to result in re-identification of participants or the production of identifiable information? If so, how?	N/A

5.4	IF YES to 5.3, how will the identity or potentially identifying information relating to original participants be safeguarded?	N/A

6. Sharing / Disseminating Results

#	Question	Answer
6.1	Describe if / how the results of this project will be shared with the research community and/or the general public.	The results of the FRAM analysis on this data will be presented in a journal publication. These results will not have potential identifiers.
6.2	If applicable, describe if / how the results of this project will be shared with participants from whom the data was originally collected, relevant agencies, or communities.	N/A

7. Funding, Contracts, and Agreements

#	Question	Answer
7.1	Please select the appropriate funding status for this project:	Funded
7.2	If funded, or funding is being sought, please indicate the funding agency/sponsor. If there are multiple sources of funding please enter each on a new line.	Lloyd's Register Foundation (LRF)
7.3	If you indicated in 7.1 that funding is being sought, specify whether or not this project will proceed if funding is not obtained.	
7.4	Will funds be administered through Memorial's Research Grant and Contract Services (RGCS) office?	Yes

7.5	If you answered NO or OTHER to 7.4, explain.	N/A
7.6	If YES to 7.4, specify the principal investigator for the associated funding AND provide the RGCS Awards file number(s):	PI is Brian Veitch and Faisal Khan. The Award title is "Scenario based risk management for Arctic shipping and operations."
7.7	Is there a funded or non-funded contract or research / partnership agreement associated with this research?	Yes
7.8	If YES to 7.7, specify the parties to the contract / agreement, and discuss the contract / agreement provisions relating to intellectual property, data access, and data ownership. Upload a copy of the agreement / contract in the Attachments tab.	See attachment

8. Conflict of Interest

#	Question	Answer
8.1	Is there any aspect of a contract/agreement that could put any member of the research team in a potential conflict of interest?	No
8.2	If YES, identify the conflict(s) and discuss how they will be mitigated.	N/A

9. Pre-Submission Checklist

#	Question	Answer
9.1	All questions have been answered in the space allowed (Including "N/A" where appropriate).	Yes
9.2	A copy of the Principal Investigator’s TCPS2 Tutorial Certificate of	Yes

	Completion is included in the Attachments tab.	
9.3	A copy of any funded or non-funded contract or research / partnership agreement is included in the Attachments tab.	Yes
9.4	A copy of the correspondence regarding data access from the data holder / custodian has been attached in the Attachments tab.	Not Applicable
9.5	If this study primarily involves data from an Aboriginal population, a copy of the research agreement or letter of support from the relevant community groups and boards is included.	No
9.6	The supervisor signature form is included. (Students Only)	Yes
9.7	(Faculty / Staff) If funded, the project funding has been linked under 'Related Awards' on the Project Info tab.	No
9.8	(Student / Postdoc) If funded, the 'Funded Projects' section has been completed on the attached Supervisor signature page.	Yes

10. Declaration

#	Question	Answer
10.1	I have read, and understand that I must comply with, Memorial University's Policy on Ethics of Research Involving Human Participants and the Tri-Council Policy Statement on Ethical Conduct for Research Involving Humans (TCPS2 - 2014).	Agree
10.2	I will ensure that all procedures performed under the project will be	Agree

	conducted in accordance with the TCPS2 (2014) and all relevant university, provincial, national, and international policies and regulations that govern the collection and use of personally identifiable information and/or any other data in research involving human participants.	
10.3	I agree to conduct the research subject to Section 3 (Guiding Ethical Principles) and accept the responsibilities as outlined in Section 18 (Responsibilities of Researchers) of Memorial University's Policy on Ethics of Research Involving Human Participants.	Agree
10.4	I understand that if I misrepresent and/or fail to accurately and fully disclose any aspects of the research, my ethics clearance may be suspended.	Agree
10.5	I understand that Article 6.16 of the TCPS2 (2014) requires that I submit an amendment request to ICEHR before making any changes to my approved protocol that may affect participants including, but not limited to, changes in recruitment, informed consent, test instruments, and/or tasks or interventions involved in the research. I understand that changes implemented without approval constitute a violation of the TCPS2 (2014) and Memorial University policy.	Agree
10.6	I understand that Article 6.14 (Continuing Research Ethics Review) of the TCPS2 (2014) requires that I submit an annual update for each year my project is active, and a final report after my project is completed.	Agree

10.7	If there is any occurrence of an adverse event(s), I will report it to ICEHR immediately by submitting an Adverse Event Report.	Agree

Attachments

Doc / Agreement	Version Date	File Name	Description
Informed Consent Form	2018/03/04	Appendix-A-Consent-Form-rev6.pdf	Original informed consent form
Other REB Application/Approval	2018/02/28	LRF_Agreement_signedMUN.PDF	N/A
Secondary Use of Data Approval Letter	2018/03/05	Data-Holder-Agreement-for-Secondary-Use.pdf	N/A
Signature Form	2018/03/01	supervisorform_ethicssigned.pdf	N/A
Signature Form	2018/03/05	supervisorform_ethicssignedrgcs.pdf	Updated supervisor's signature page
TCPS2 Certificate	2018/02/28	TCPSComplete_doug.pdf	N/A

TCPS2 Certificate	2018/03/05	tcps2_core_certificate.pdf	Supervisor's tcps2 core certificate

8. Appendix B

Name of function	Controlled Propane Flow
Description	The main function of the is to supply propane in a controlled manner
Aspect	Description of aspect
Input	Feed controlled automatically
	Feed controlled manually
Output	
Precondition	
Resource	
Control	
Time	

Name of function	Manually Operate Valve
Description	The valve is adjusted manually in the event that the automatic system is not functioning

Aspect	Description of aspect
Input	Manual intervention needed
Output	Feed controlled manually
Precondition	Worker available
Resource	
Control	
Time	

Name of function	Automatically Operate Valve
Description	Actuator adjusts valve automatically to achieve desired flow rate
Aspect	Description of aspect
Input	Voltage relayed
Output	Feed controlled automatically
Precondition	
Resource	
Control	
Time	

Name of function	Delegate Worker Responsibility

Description	Management must delegate worker(s) to be responsible for monitoring the automatic system and operating the manual valve
Aspect	Description of aspect
Input	
Output	Worker available
Precondition	
Resource	
Control	
Time	

Name of function	Alert Worker
Description	Alarm sounds to alert worker when it is detected that automatic control is not functioning properly
Aspect	Description of aspect
Input	Feed controlled automatically
Output	Worker Alerted

Precondition	
Resource	
Control	
Time	

Name of function	Relay pressure
Description	Relays the pressure difference (voltage signal) to the actuator
Aspect	Description of aspect
Input	Pressure controlled
Output	Voltage relayed
Precondition	
Resource	
Control	
Time	

Name of function	Set Desired Flow Rate
Description	Calibrate the pressure controller to send required voltage to actuator to adjust automatic valve to achieve desired flow rate after pressure measurement

Aspect	Description of aspect
Input	
Output	Set flow rate
Precondition	
Resource	
Control	
Time	

Name of function	Measure Pressure
Description	Pressure sensor measures the pressure and sends to the pressure controller
Aspect	Description of aspect
Input	
Output	Pressure measured
Precondition	
Resource	
Control	
Time	

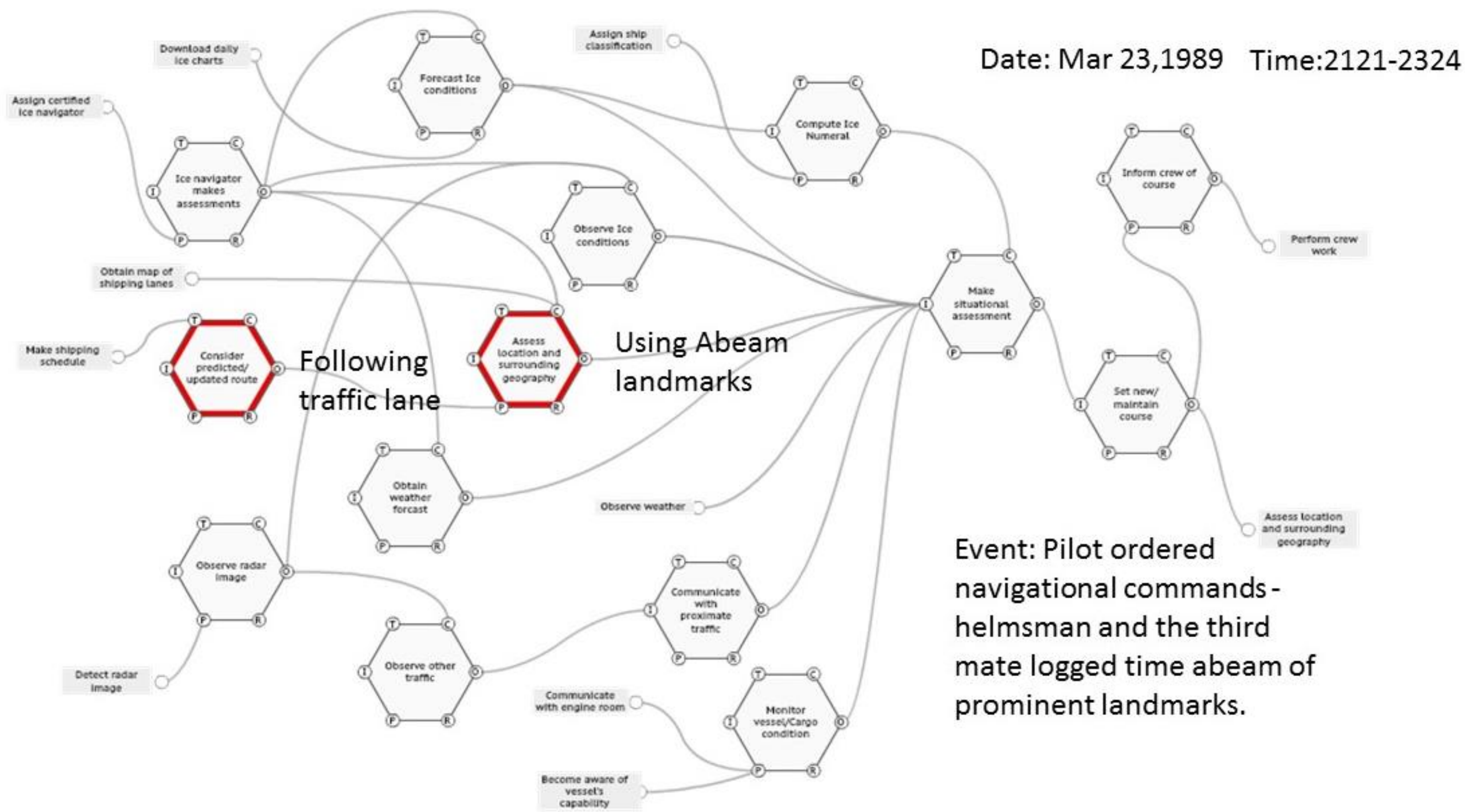
Name of function	Control Pressure

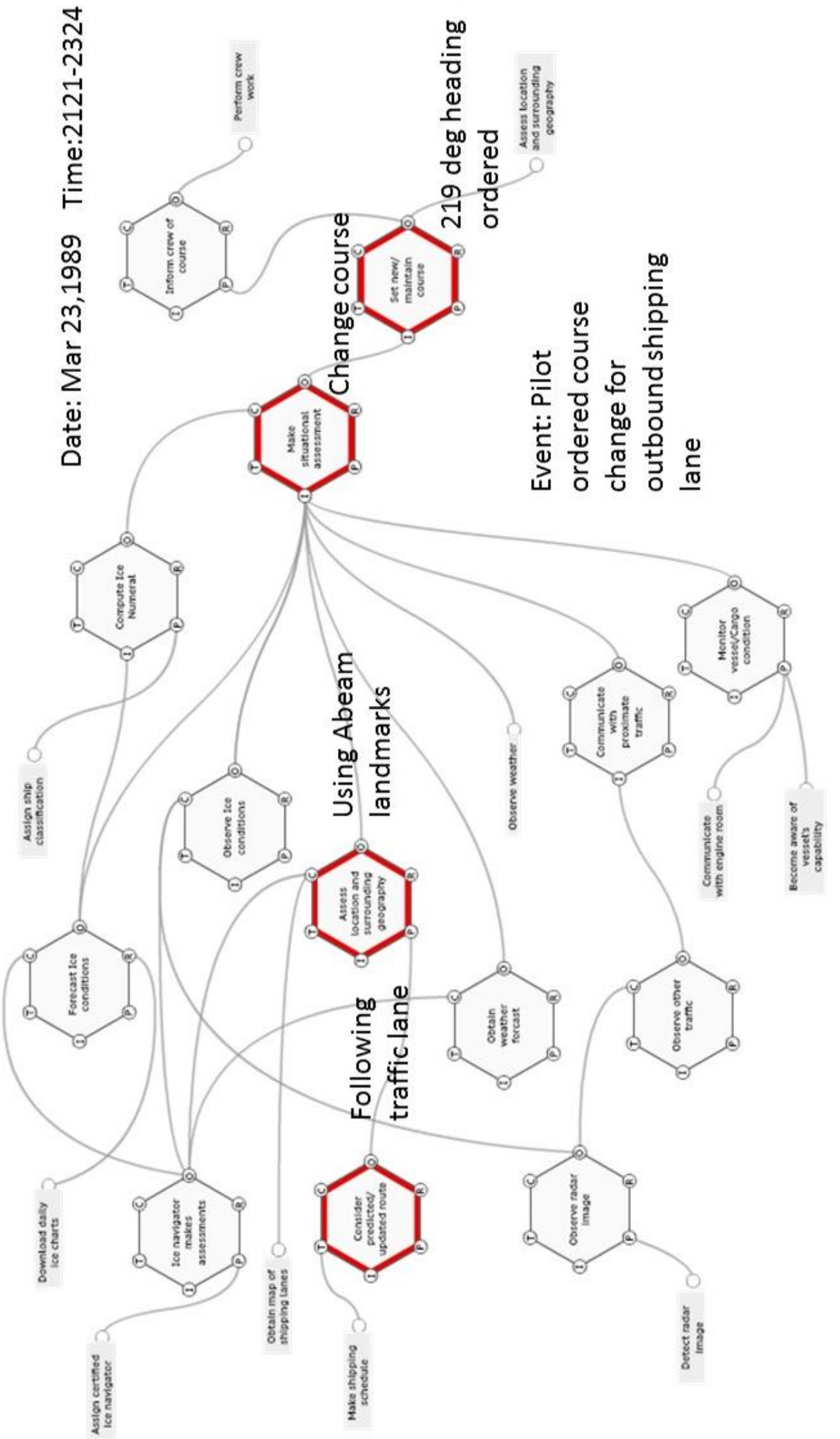
Description	Measured pressure is compared with desired pressure by the pressure controller
Aspect	Description of aspect
Input	Pressure measured
Output	Pressure controlled
Precondition	
Resource	
Control	Set flow rate
Time	

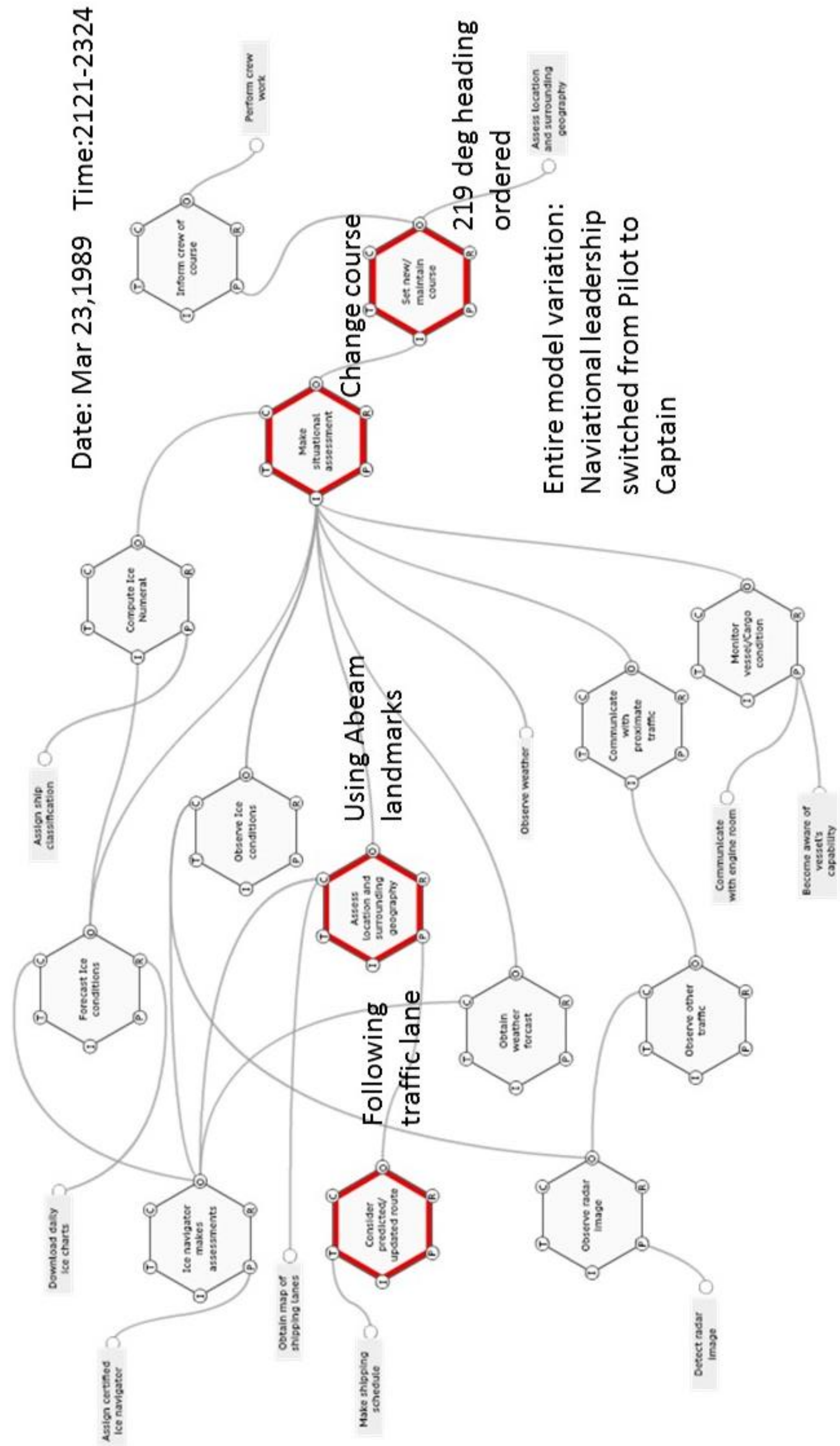
Name of function	Monitor Automatic System
Description	A worker must monitor the automatic control system to ensure it is functioning properly
Aspect	Description of aspect
Input	Feed controlled automatically
Output	Manual intervention needed
Precondition	Worker available
Resource	
Control	Set flow rate

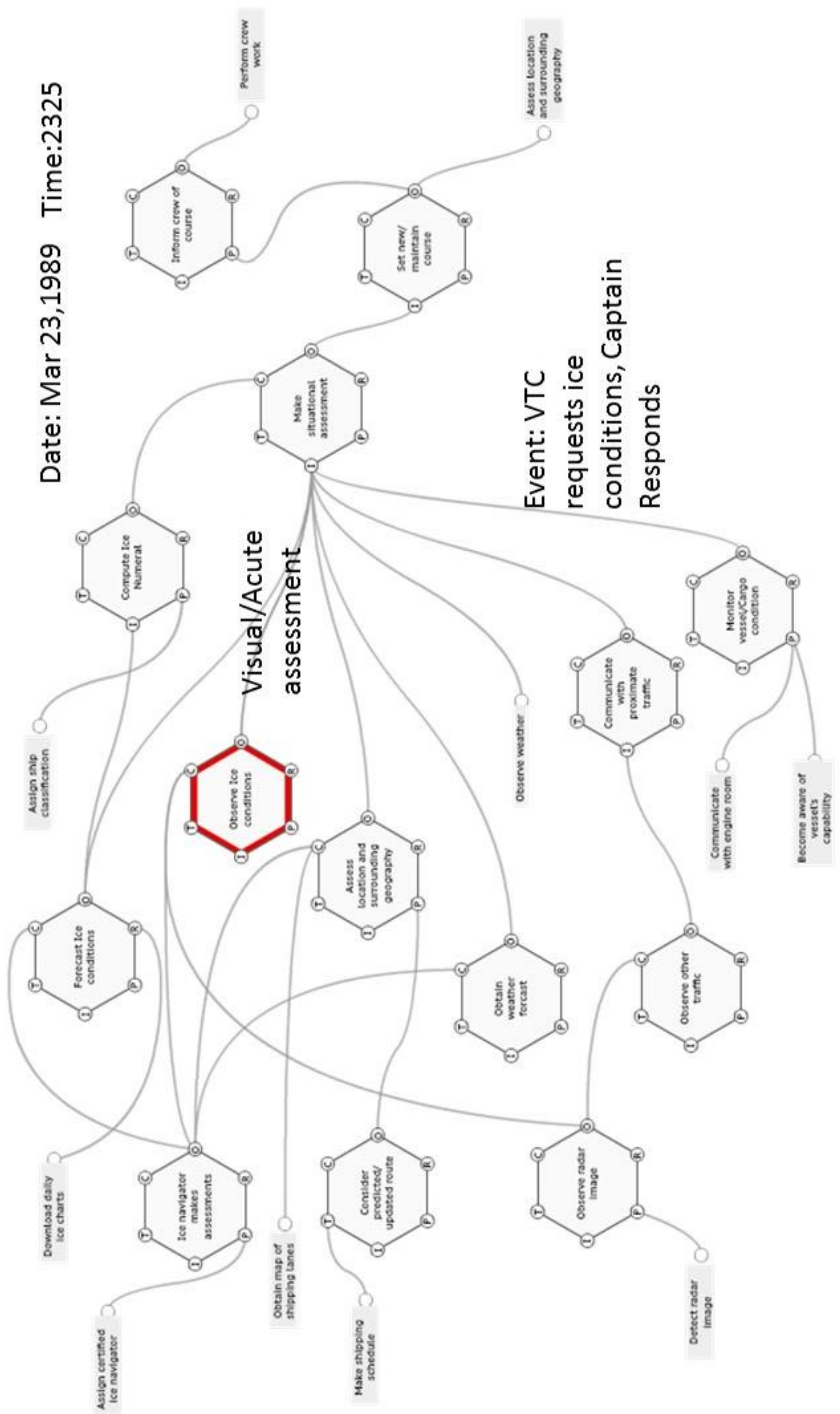
Time	Worker Alerted

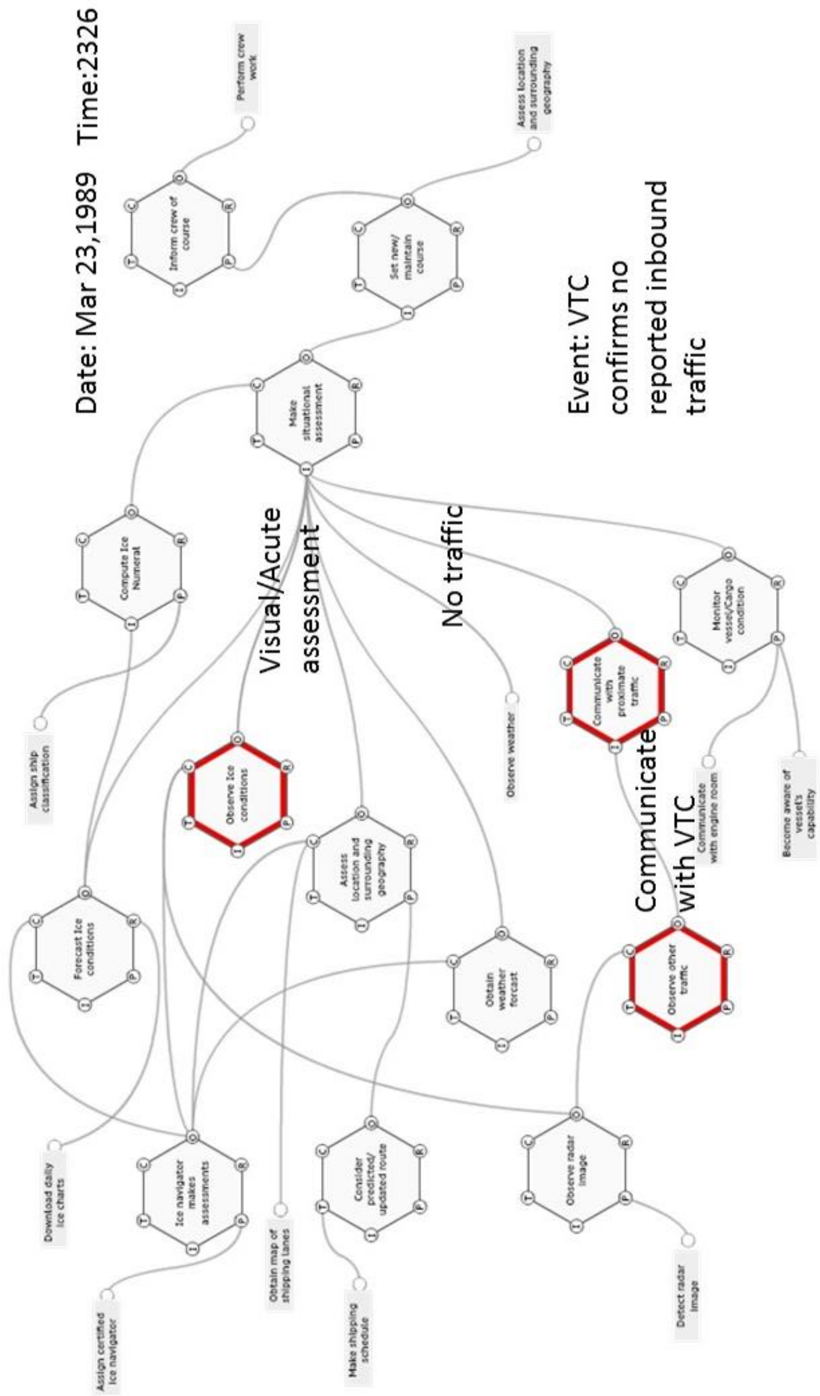
9. Appendix C


Date: Mar 23,1989 Time:2121-2324
Download daily ice charts
Assign certified ice navigator
Forecast Ice conditions
Assign ship classification
Compute Ice Numeral
Inform crew of course
Perform crew work
Ice navigator makes assessments
Observe Ice conditions
Obtain map of shipping lanes
Make situational assessment
Make shipping schedule
Consider predicted/ updated route
Following traffic lane
Assess location and surrounding geography
Using Abeam landmarks
Set new/ maintain course
Obtain weather forcast
Observe weather
Assess location and surrounding geography
Observe radar image
Event: Pilot ordered navigational commands - helmsman and the third mate logged time abeam of prominent landmarks.
Communicate with proximate traffic
Detect radar image
Observe other traffic
Communicate with engine room
Monitor vessel/Cargo condition
Become aware of vessel's capability

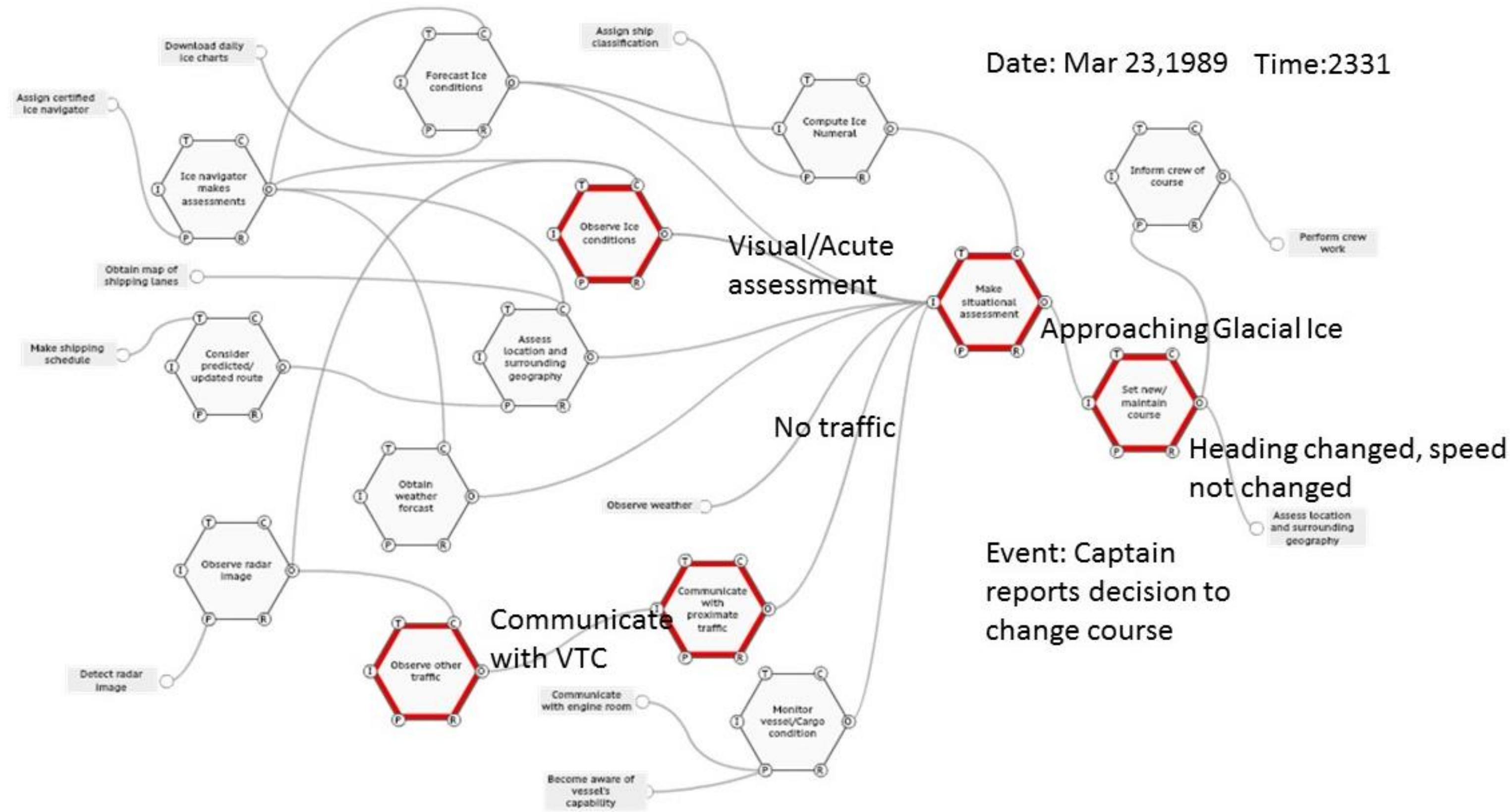

Date: Mar 23,1989 Time:2121-2324
219 deg heading ordered
Change course
Event: Pilot ordered course change for outbound shipping lane
Using Abeam landmarks
Following traffic lane
Perform crew work
Inform crew of course
Assess location and surrounding geography
Set new/ maintain course
Make situational assessment
Compute Ice Numeral
Assign ship classification
Observe Ice conditions
Observe weather
Communicate with proximate traffic
Monitor vessel/Cargo condition
Communicate with engine room
Become aware of vessel's capability
Assess location and surrounding geography
Forecast Ice conditions
Obtain weather forcast
Observe other traffic
Download daily ice charts
Ice navigator makes assessments
Obtain map of shipping lanes
Consider predicted/ updated route
Observe radar image
Detect radar image
Make shipping schedule
Assign certified ice navigator


Date: Mar 23,1989 Time:2121-2324
Change course
219 deg heading ordered
Entire model variation: Naviational leadership switched from Pilot to Captain
Using Abeam landmarks
Following traffic lane
Perform crew work
Inform crew of course
Set new/ maintain course
Assess location and surrounding geography
Make situational assessment
Compute Ice Numeral
Assign ship classification
Observe Ice conditions
Observe weather
Communicate with proximate traffic
Monitor vessel/Cargo condition
Communicate with engine room
Become aware of vessel's capability
Forecast Ice conditions
Obtain weather forcast
Observe other traffic
Download daily ice charts
Ice navigator makes assessments
Obtain map of shipping lanes
Consider predicted/ updated route
Observe radar image
Detect radar image
Assign certified ice navigator
Make shipping schedule

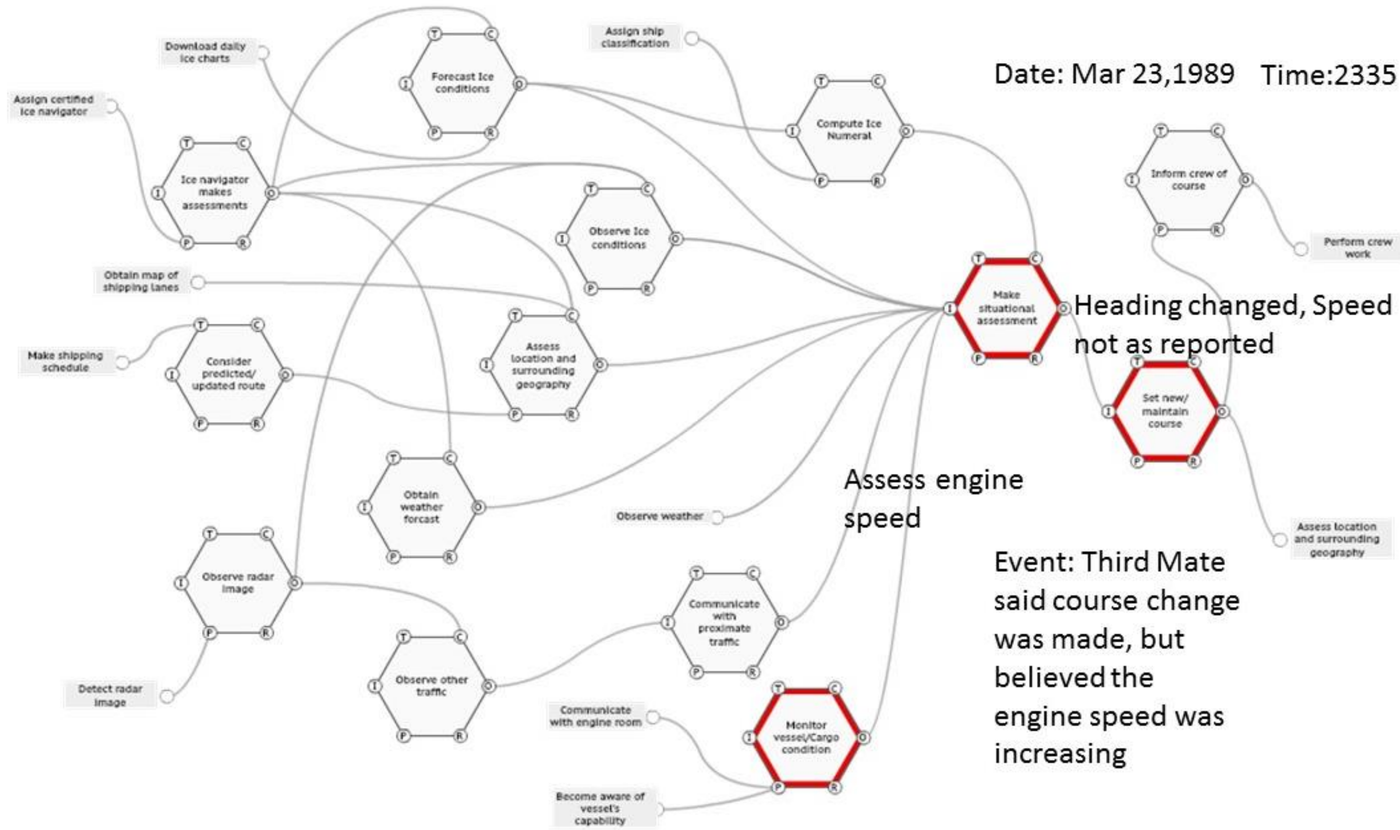

Date: Mar 23,1989 Time:2325
Event: VTC requests ice conditions, Captain Responds
Visual/Acute assessment
Perform crew work
Assess location and surrounding geography
Inform crew of course
Set new/ maintain course
Make situational assessment
Compute Ice Numeral
Monitor vessel/Cargo condition
Communicate with proximate traffic
Observe weather
Assign ship classification
Observe Ice conditions
Assess location and surrounding geography
Communicate with engine room
Become aware of vessel's capability
Forecast Ice conditions
Obtain weather forcast
Observe other traffic
Download daily ice charts
Ice navigator makes assessments
Obtain map of shipping lanes
Consider predicted/ updated route
Observe radar image
Detect radar image
Assign certified ice navigator
Make shipping schedule



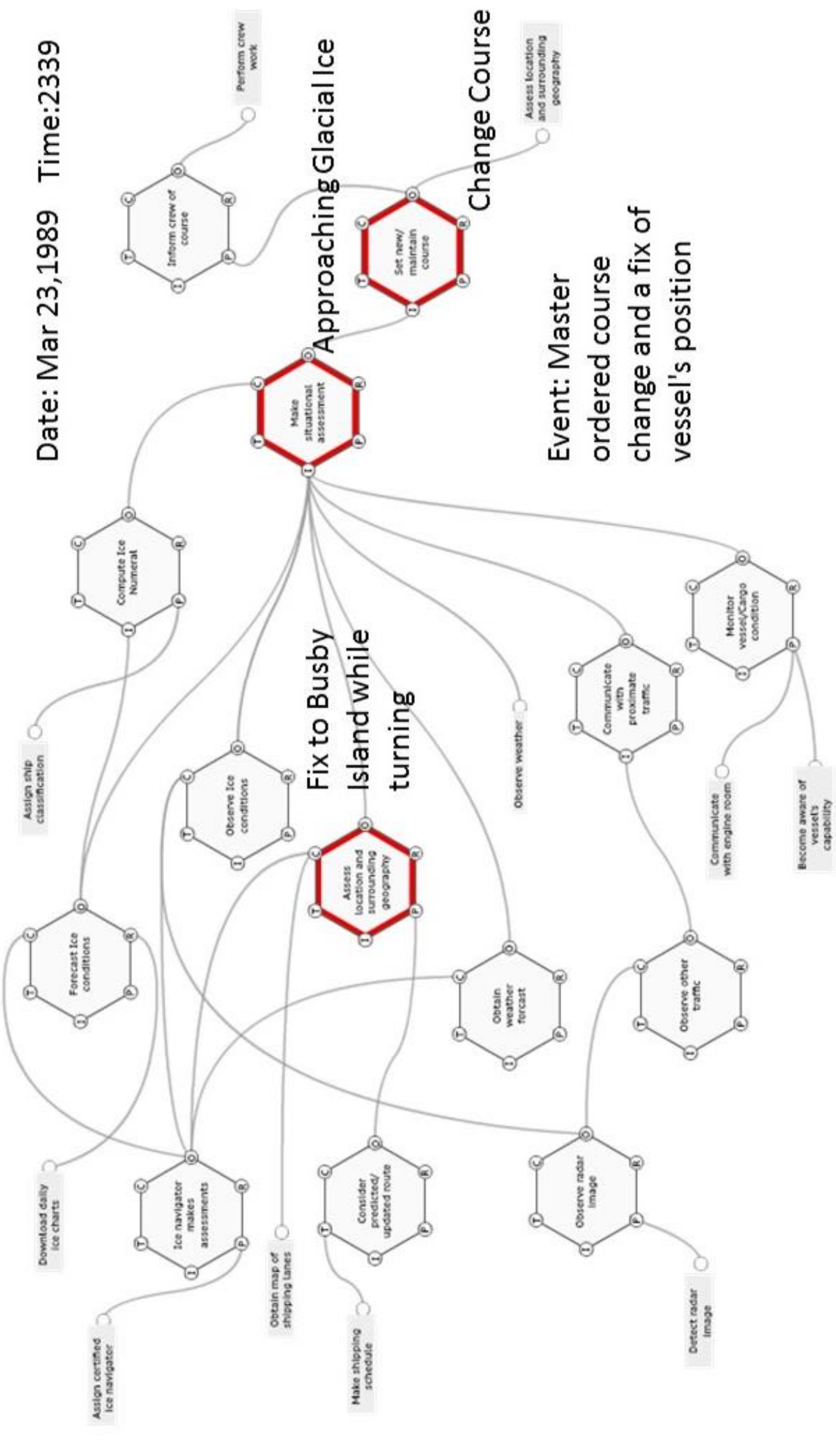
Date: Mar 23,1989
Time:2326
Event: VTC confirms no reported inbound traffic
Visual/Acute assessment
No traffic
Communicate with VTC
Perform crew work
Assess location and surrounding geography
Inform crew of course
Set new/ maintain course
Make situational assessment
Compute Ice Numeral
Monitor vessel/Cargo condition
Communicate with proximate traffic
Assign ship classification
Observe Ice conditions
Observe weather
Communicate with engine room
Become aware of vessel's capability
Assess location and surrounding geography
Forecast Ice conditions
Obtain weather forcast
Observe other traffic
Download daily ice charts
Ice navigator makes assessments
Consider predicted/ updated route
Observe radar image
Obtain map of shipping lanes
Detect radar image
Assign certified ice navigator
Make shipping schedule

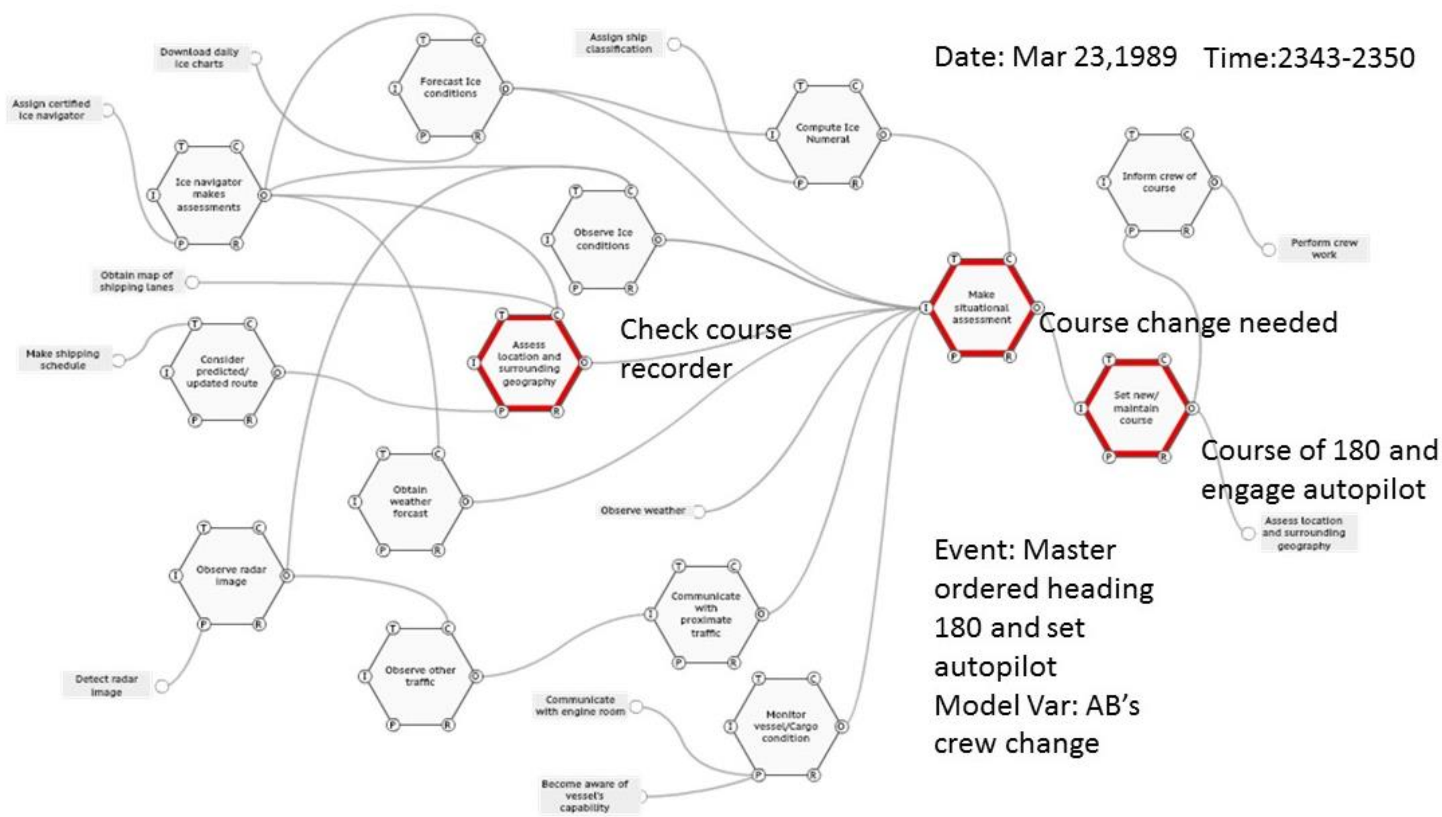


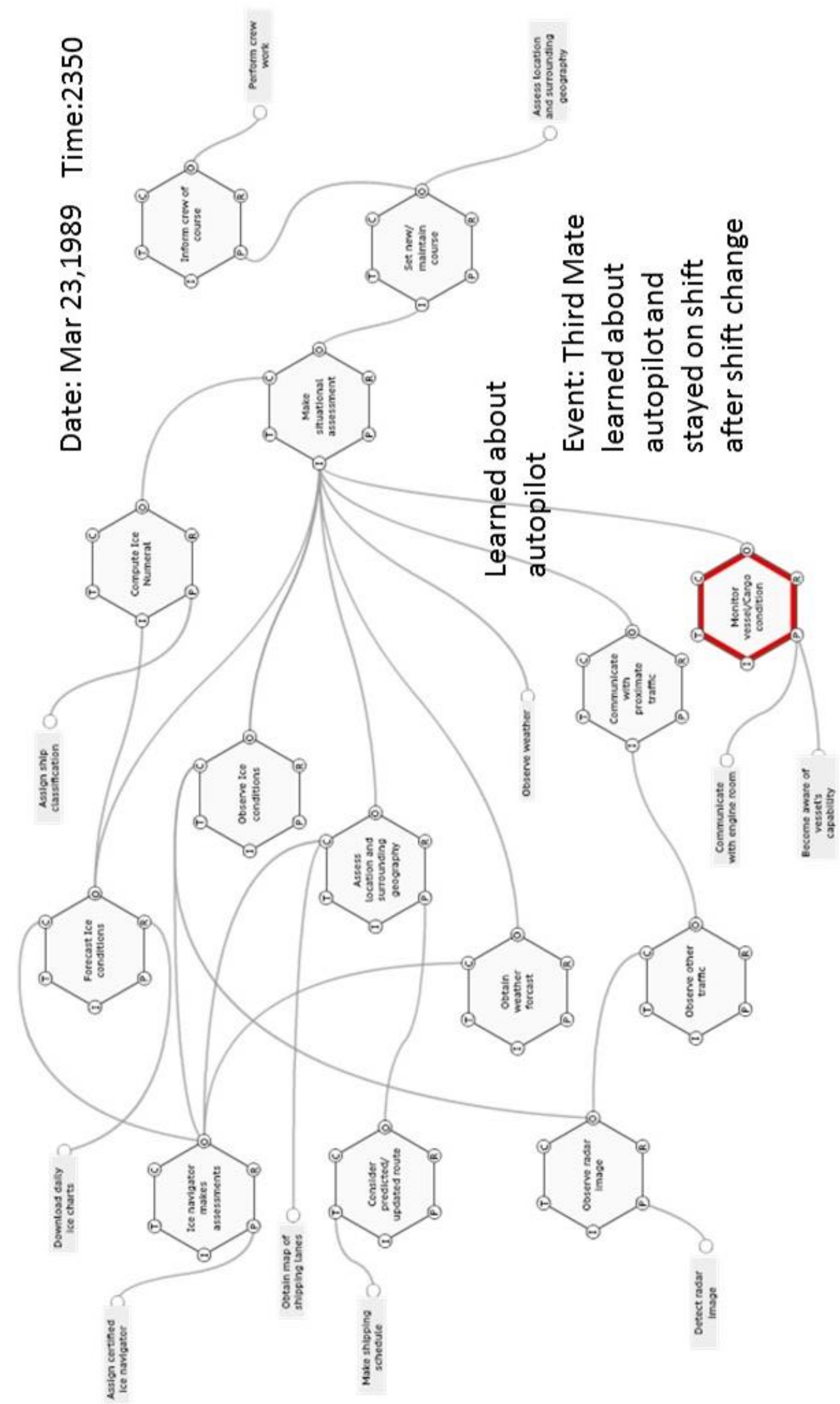
Date: Mar 23,1989 Time:2331
Event: Captain reports decision to change course
Approaching Glacial Ice
Heading changed, speed not changed
Visual/Acute assessment
No traffic
Communicate with VTC
Make situational assessment
Set new/ maintain course
Inform crew of course
Perform crew work
Assess location and surrounding geography
Compute Ice Numeral
Assign ship classification
Forecast Ice conditions
Download daily ice charts
Ice navigator makes assessments
Assign certified ice navigator
Observe Ice conditions
Obtain map of shipping lanes
Consider predicted/ updated route
Make shipping schedule
Obtain weather forcast
Observe weather
Observe radar image
Detect radar image
Observe other traffic
Communicate with proximate traffic
Monitor vessel/Cargo condition
Communicate with engine room
Become aware of vessel's capability

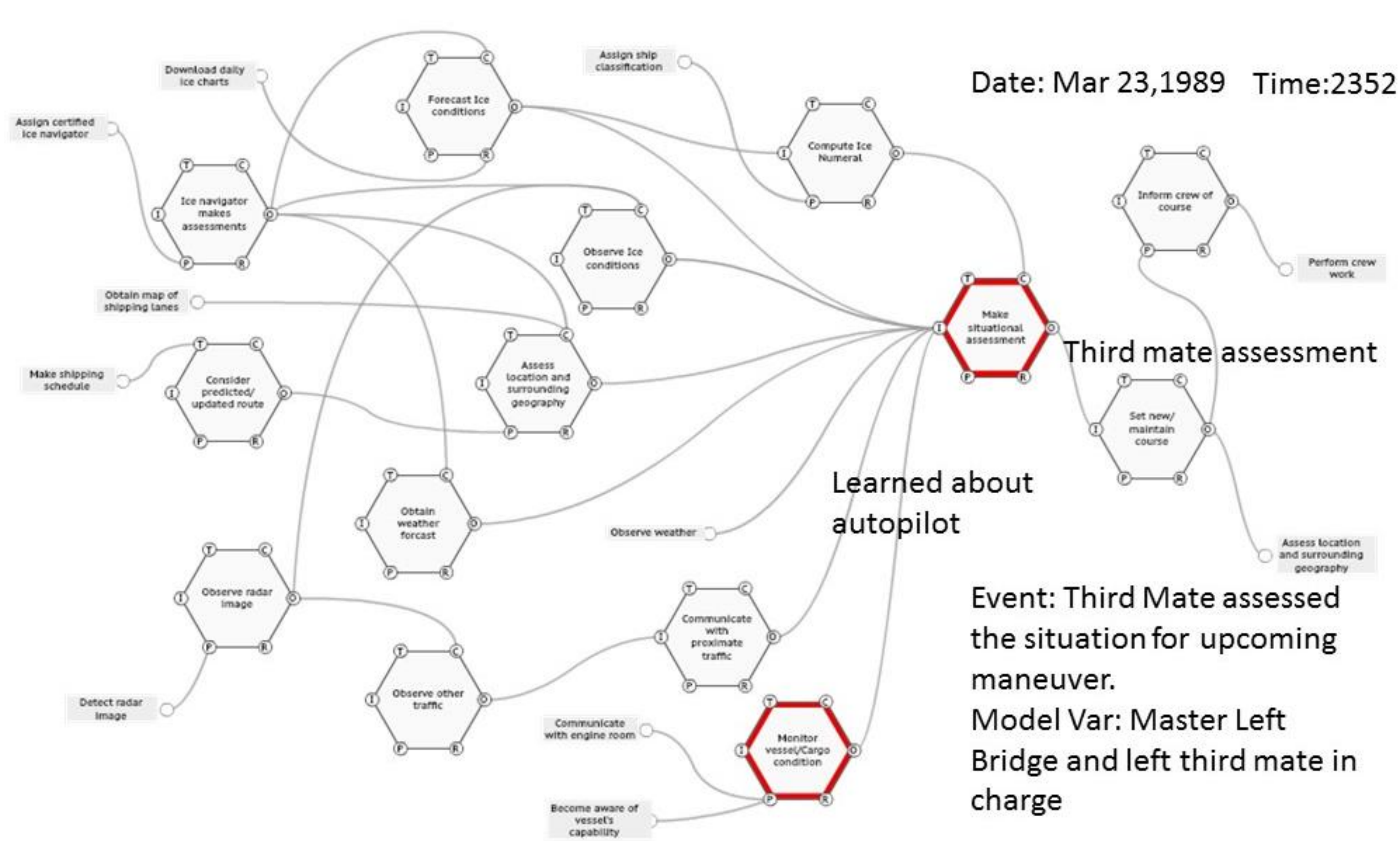


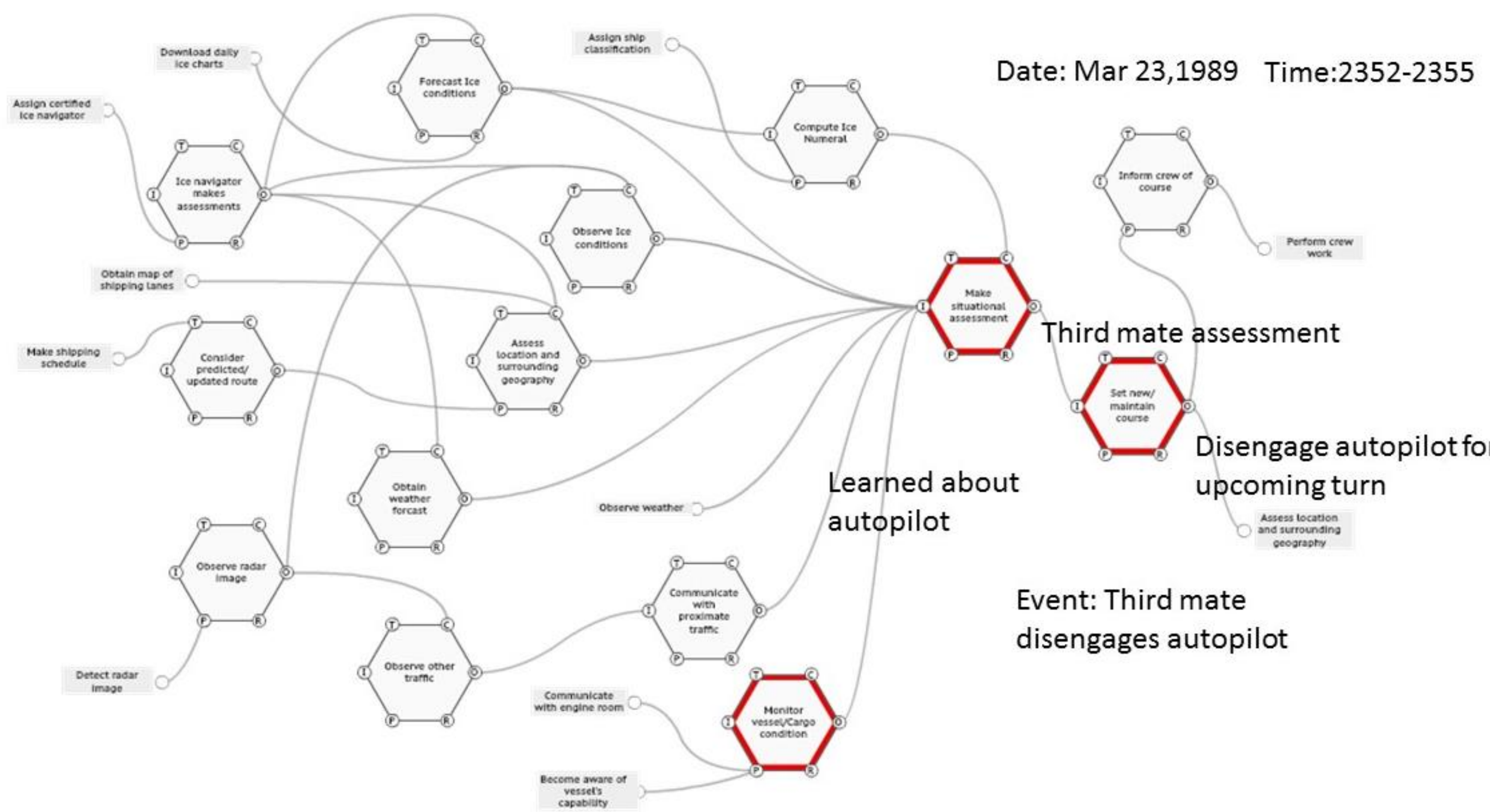
Date: Mar 23,1989 Time:2335
Heading changed, Speed not as reported
Assess engine speed
Event: Third Mate said course change was made, but believed the engine speed was increasing
Download daily ice charts
Assign certified ice navigator
Forecast Ice conditions
Assign ship classification
Compute Ice Numeral
Inform crew of course
Perform crew work
Ice navigator makes assessments
Observe Ice conditions
Obtain map of shipping lanes
Make situational assessment
Make shipping schedule
Consider predicted/ updated route
Assess location and surrounding geography
Set new/ maintain course
Obtain weather forcast
Observe weather
Assess location and surrounding geography
Observe radar image
Communicate with proximate traffic
Detect radar image
Observe other traffic
Communicate with engine room
Monitor vessel/Cargo condition
Become aware of vessel's capability

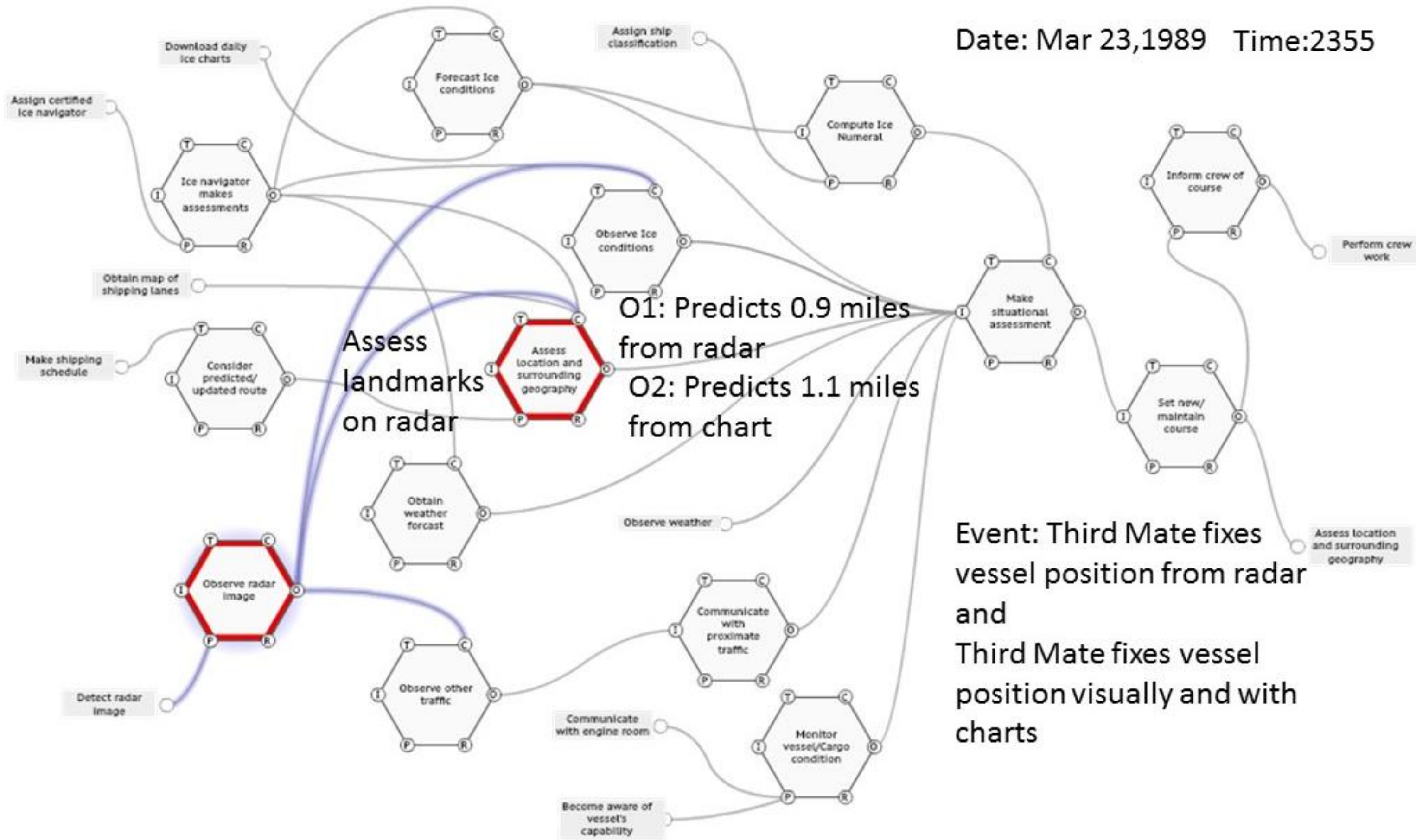

Date: Mar 23,1989 Time:2339
Approaching Glacial Ice
Change Course
Event: Master ordered course change and a fix of vessel's position
Fix to Busby Island while turning
Perform crew work
Inform crew of course
Set new/ maintain course
Assess location and surrounding geography
Make situational assessment
Compute Ice Numeral
Monitor vessel/Cargo condition
Communicate with proximate traffic
Observe weather
Assign ship classification
Observe Ice conditions
Communicate with engine room
Become aware of vessel's capability
Assess location and surrounding geography
Forecast Ice conditions
Obtain weather forcast
Observe other traffic
Download daily ice charts
Ice navigator makes assessments
Consider predicted/ updated route
Observe radar image
Obtain map of shipping lanes
Make shipping schedule
Detect radar image
Assign certified ice navigator

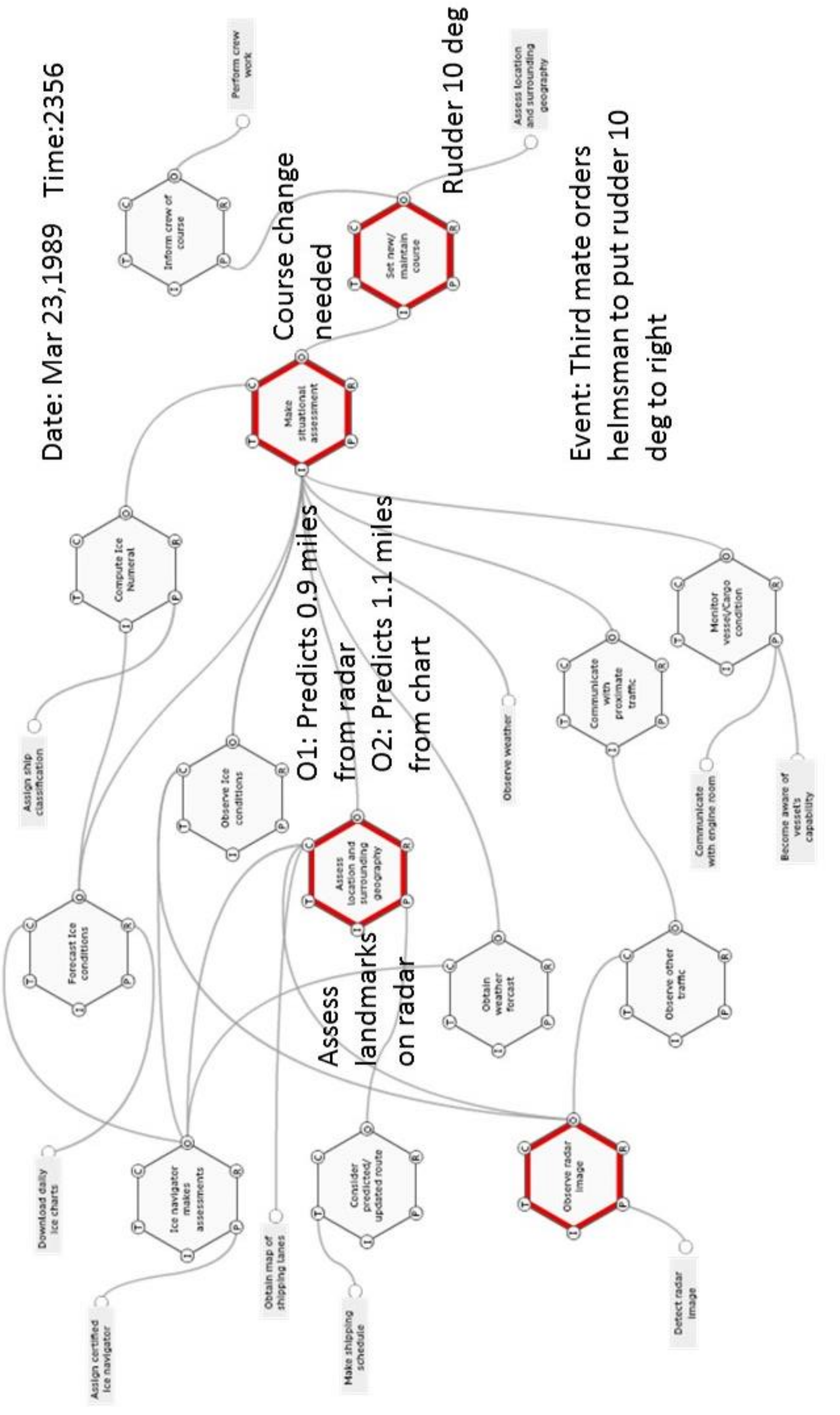

Date: Mar 23,1989 Time:2343-2350
Download daily ice charts
Forecast Ice conditions
Assign ship classification
Compute Ice Numeral
Assign certified ice navigator
Ice navigator makes assessments
Observe Ice conditions
Inform crew of course
Perform crew work
Obtain map of shipping lanes
Make situational assessment
Course change needed
Assess location and surrounding geography
Check course recorder
Make shipping schedule
Consider predicted/ updated route
Set new/ maintain course
Course of 180 and engage autopilot
Obtain weather forcast
Observe weather
Assess location and surrounding geography
Observe radar image
Event: Master ordered heading 180 and set autopilot
Model Var: AB's crew change
Communicate with proximate traffic
Observe other traffic
Detect radar image
Communicate with engine room
Monitor vessel/Cargo condition
Become aware of vessel's capability

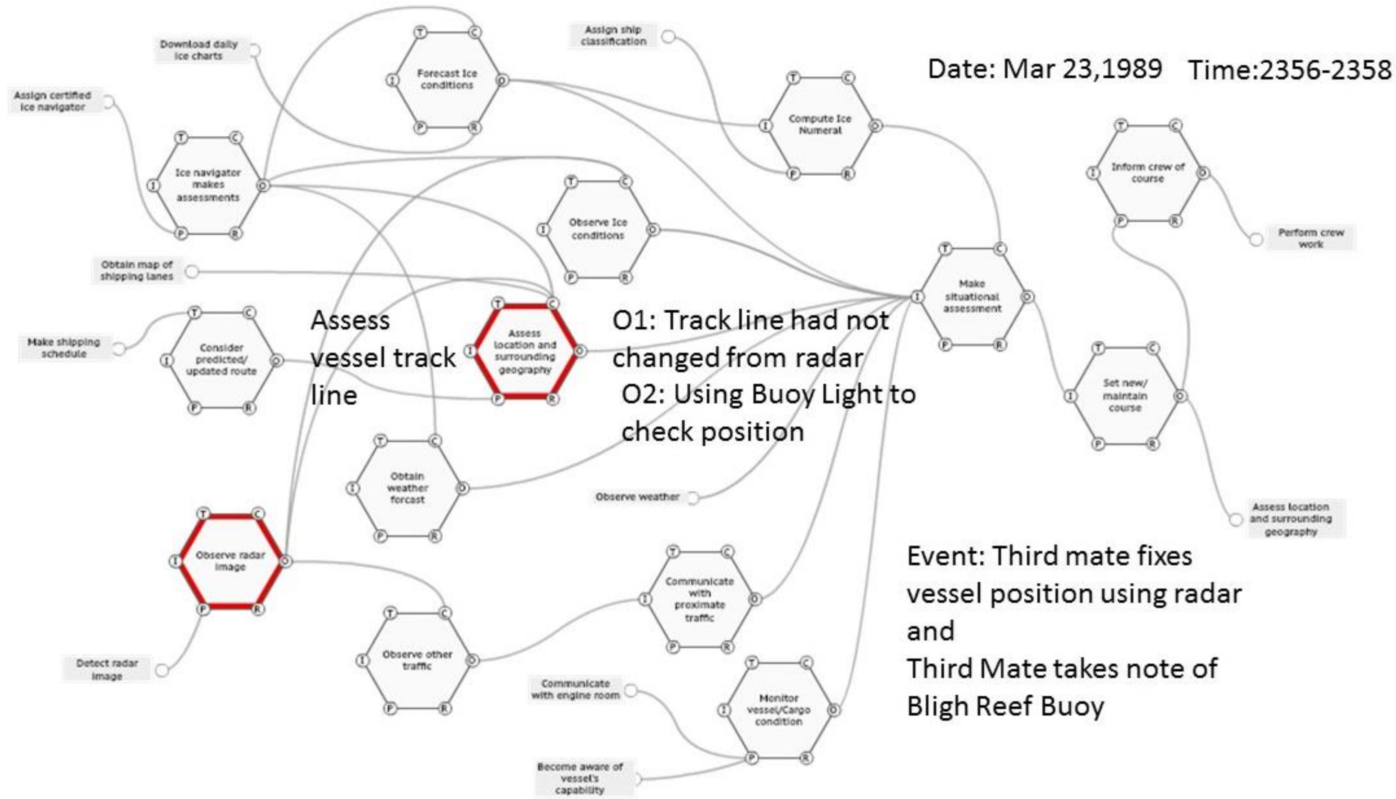

Date: Mar 23,1989 Time:2350
Event: Third Mate learned about autopilot and stayed on shift after shift change
Learned about autopilot
Perform crew work
Inform crew of course
Assess location and surrounding geography
Set new/ maintain course
Make situational assessment
Compute Ice Numeral
Monitor vessel/Cargo condition
Communicate with proximate traffic
Assign ship classification
Observe weather
Communicate with engine room
Become aware of vessel's capability
Observe Ice conditions
Assess location and surrounding geography
Forecast Ice conditions
Obtain weather forcast
Observe other traffic
Download daily ice charts
Ice navigator makes assessments
Obtain map of shipping lanes
Consider predicted/ updated route
Observe radar image
Detect radar image
Assign certified ice navigator
Make shipping schedule

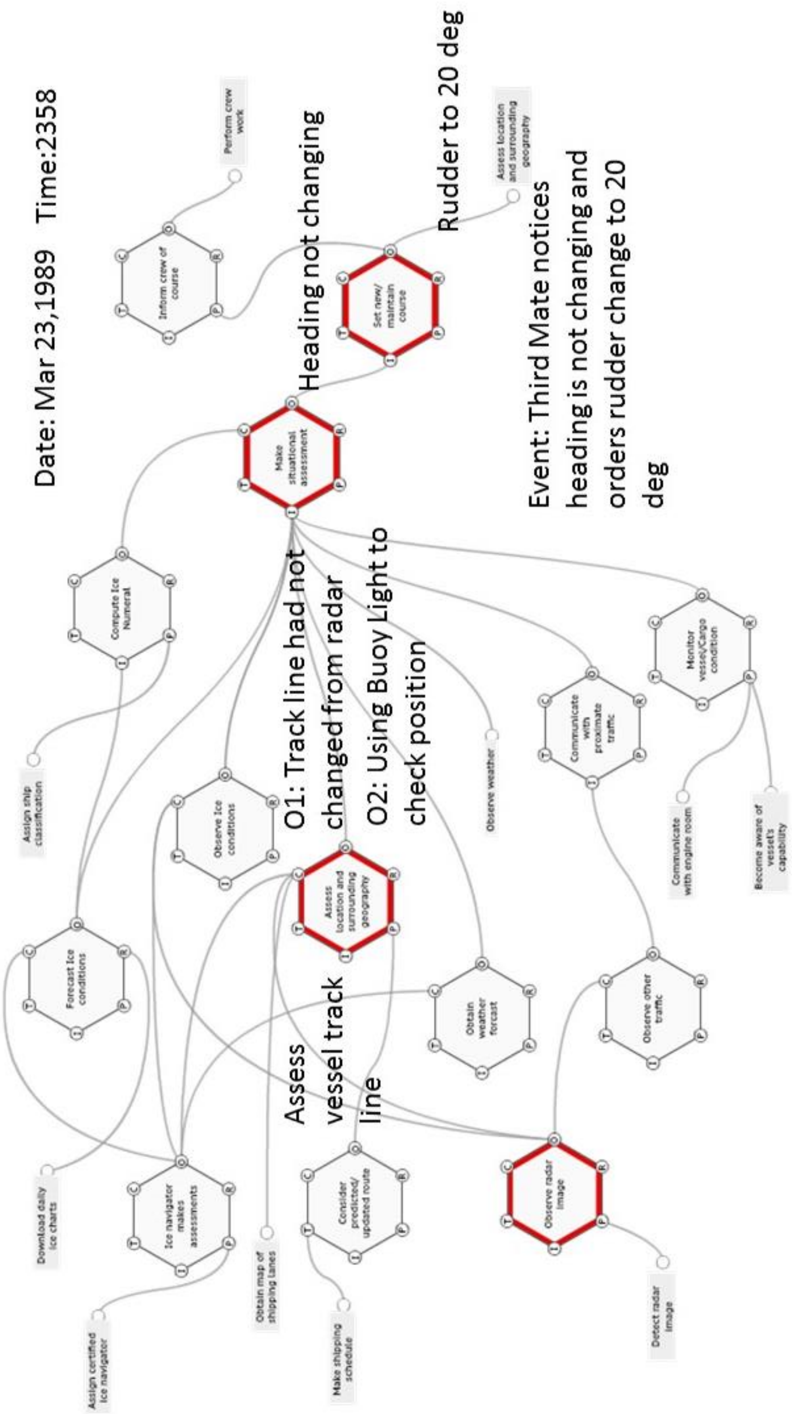

Date: Mar 23,1989 Time:2352
Download daily ice charts
Assign certified ice navigator
Forecast Ice conditions
Assign ship classification
Compute Ice Numeral
Inform crew of course
Perform crew work
Ice navigator makes assessments
Observe Ice conditions
Obtain map of shipping lanes
Make situational assessment
Third mate assessment
Make shipping schedule
Consider predicted/ updated route
Assess location and surrounding geography
Set new/ maintain course
Learned about autopilot
Obtain weather forcast
Observe weather
Assess location and surrounding geography
Observe radar image
Communicate with proximate traffic
Event: Third Mate assessed the situation for upcoming maneuver.
Model Var: Master Left Bridge and left third mate in charge
Detect radar image
Observe other traffic
Communicate with engine room
Monitor vessel/Cargo condition
Become aware of vessel's capability

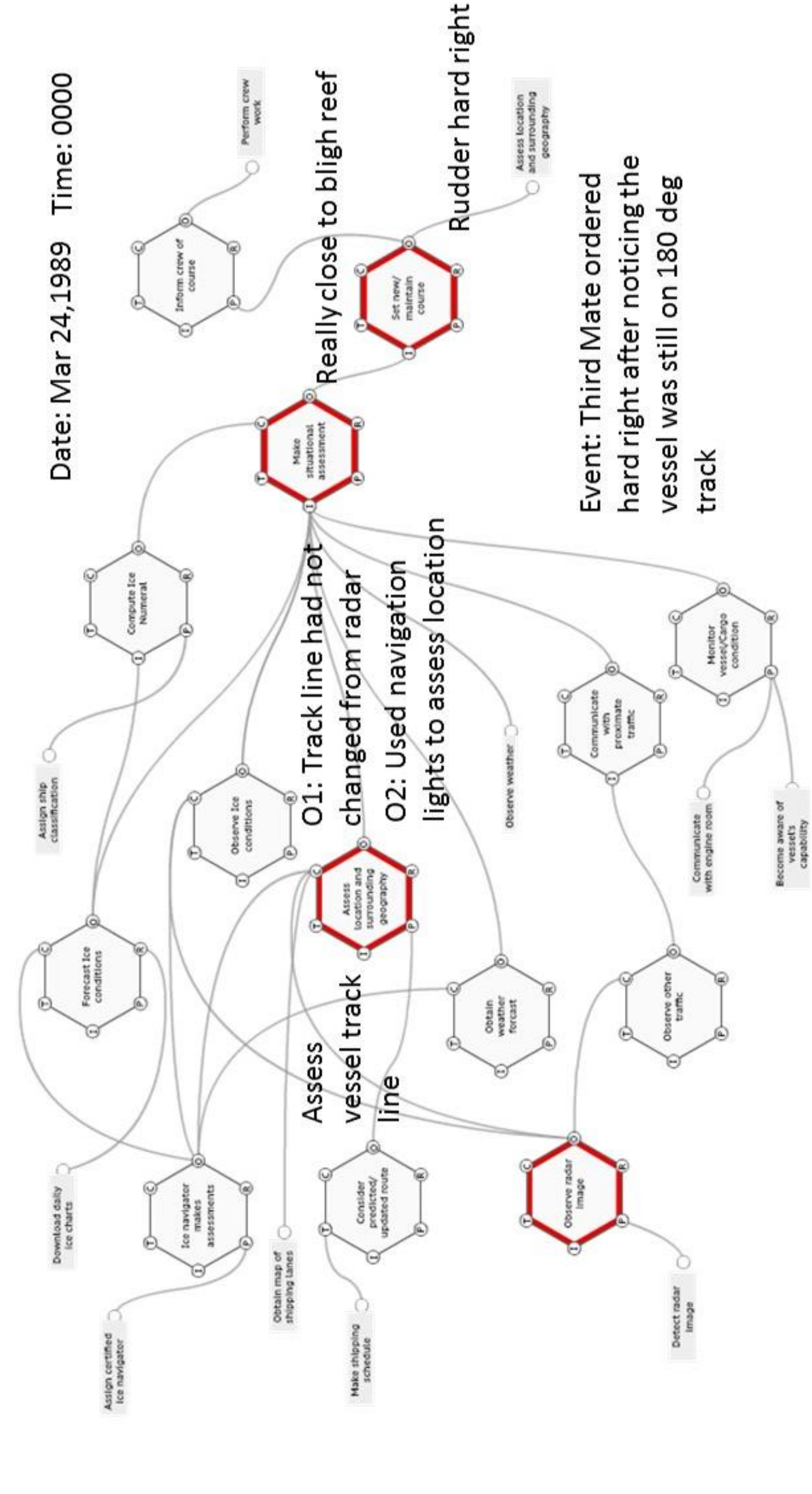

Date: Mar 23,1989 Time:2352-2355
Third mate assessment
Disengage autopilot for upcoming turn
Learned about autopilot
Event: Third mate disengages autopilot
Make situational assessment
Set new/ maintain course
Inform crew of course
Perform crew work
Assess location and surrounding geography
Compute Ice Numeral
Assign ship classification
Forecast Ice conditions
Download daily ice charts
Assign certified ice navigator
Ice navigator makes assessments
Observe Ice conditions
Obtain map of shipping lanes
Assess location and surrounding geography
Make shipping schedule
Consider predicted/ updated route
Obtain weather forcast
Observe weather
Observe radar image
Detect radar image
Observe other traffic
Communicate with proximate traffic
Communicate with engine room
Monitor vessel/Cargo condition
Become aware of vessel's capability

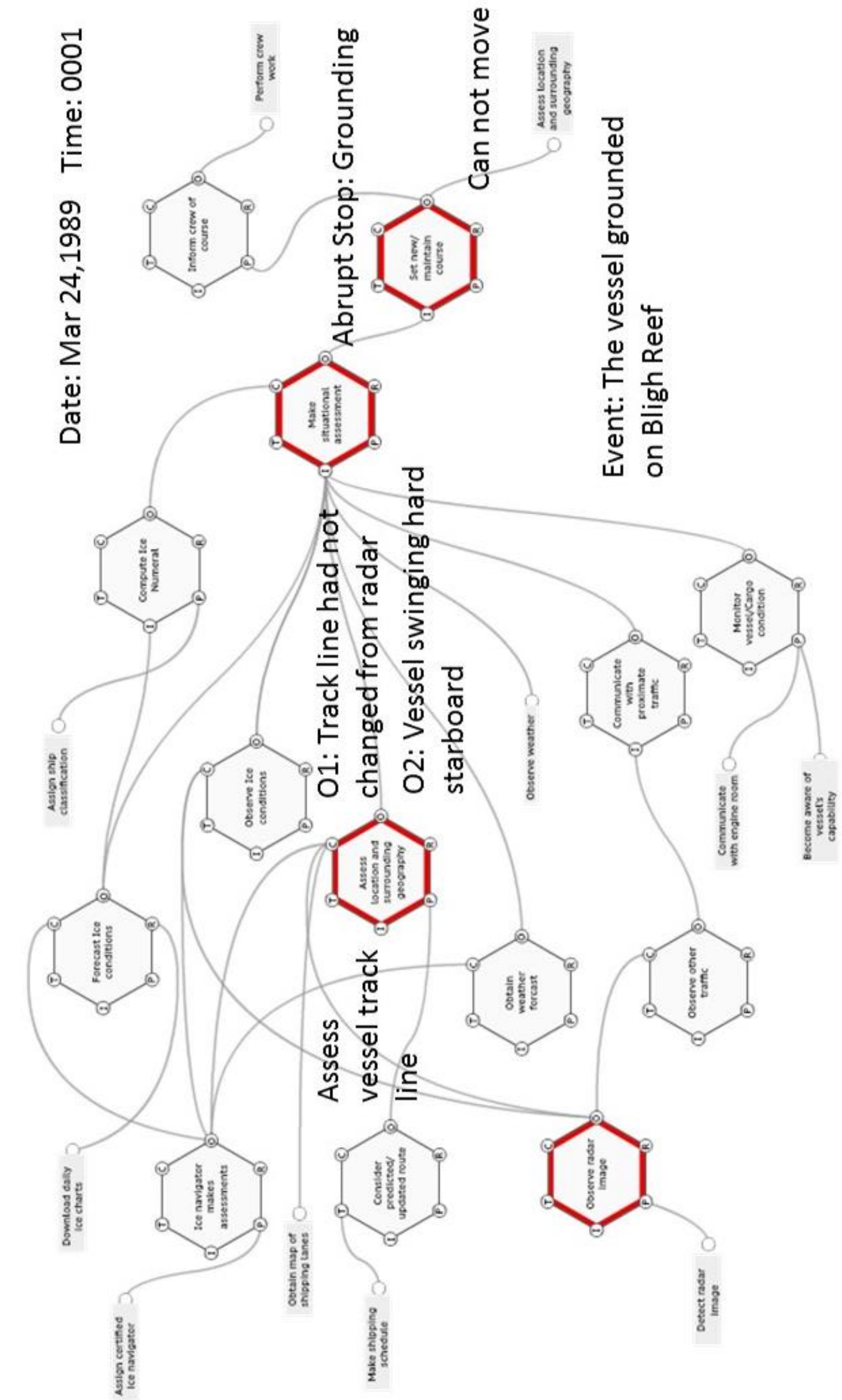

Date: Mar 23,1989 Time:2355
Event: Third Mate fixes vessel position from radar and Third Mate fixes vessel position visually and with charts
O1: Predicts 0.9 miles from radar
O2: Predicts 1.1 miles from chart
Assess landmarks on radar
Download daily ice charts
Forecast Ice conditions
Assign ship classification
Compute Ice Numeral
Assign certified ice navigator
Ice navigator makes assessments
Observe Ice conditions
Inform crew of course
Perform crew work
Obtain map of shipping lanes
Make situational assessment
Make shipping schedule
Consider predicted/ updated route
Assess location and surrounding geography
Set new/ maintain course
Obtain weather forcast
Observe weather
Assess location and surrounding geography
Observe radar image
Communicate with proximate traffic
Detect radar image
Observe other traffic
Communicate with engine room
Monitor vessel/Cargo condition
Become aware of vessel's capability


Date: Mar 23,1989 Time:2356
Course change needed
Rudder 10 deg
Event: Third mate orders helmsman to put rudder 10 deg to right
O1: Predicts 0.9 miles from radar
O2: Predicts 1.1 miles from chart
Assess landmarks on radar
Perform crew work
Inform crew of course
Set new/ maintain course
Assess location and surrounding geography
Make situational assessment
Compute Ice Numeral
Assign ship classification
Observe Ice conditions
Observe weather
Communicate with proximate traffic
Monitor vessel/Cargo condition
Communicate with engine room
Become aware of vessel's capability
Forecast Ice conditions
Assess location and surrounding geography
Obtain weather forcast
Observe other traffic
Download daily ice charts
Ice navigator makes assessments
Assign certified ice navigator
Obtain map of shipping lanes
Consider predicted/ updated route
Make shipping schedule
Observe radar image
Detect radar image


Date: Mar 23,1989 Time:2356-2358
Download daily ice charts
Assign certified ice navigator
Forecast Ice conditions
Assign ship classification
Compute Ice Numeral
Inform crew of course
Perform crew work
Ice navigator makes assessments
Observe Ice conditions
Make situational assessment
Obtain map of shipping lanes
Assess location and surrounding geography
Make shipping schedule
Consider predicted/ updated route
Assess
vessel track
line
O1: Track line had not
changed from radar
O2: Using Buoy Light to
check position
Set new/ maintain course
Obtain weather forcast
Observe weather
Assess location and surrounding geography
Observe radar image
Event: Third mate fixes
vessel position using radar
and
Third Mate takes note of
Bligh Reef Buoy
Communicate with proximate traffic
Detect radar image
Observe other traffic
Communicate with engine room
Monitor vessel/Cargo condition
Become aware of vessel's capability


Date: Mar 23,1989 Time:2358
Perform crew work
Inform crew of course
Heading not changing
Set new/ maintain course
Rudder to 20 deg
Assess location and surrounding geography
Event: Third Mate notices heading is not changing and orders rudder change to 20 deg
Make situational assessment
Compute Ice Numeral
O1: Track line had not changed from radar
O2: Using Buoy Light to check position
Monitor vessel/Cargo condition
Communicate with proximate traffic
Observe weather
Assign ship classification
Observe Ice conditions
Communicate with engine room
Become aware of vessel's capability
Assess location and surrounding geography
Forecast Ice conditions
Obtain weather forcast
Observe other traffic
Assess vessel track line
Download daily ice charts
Ice navigator makes assessments
Consider predicted/ updated route
Observe radar image
Obtain map of shipping lanes
Detect radar image
Assign certified ice navigator
Make shipping schedule


Date: Mar 24,1989   Time: 0000
Really close to bligh reef
Rudder hard right
Event: Third Mate ordered hard right after noticing the vessel was still on 180 deg track
O1: Track line had not changed from radar
O2: Used navigation lights to assess location
Assess vessel track line
Perform crew work
Inform crew of course
Assess location and surrounding geography
Set new/ maintain course
Make situational assessment
Compute Ice Numeral
Assign ship classification
Observe Ice conditions
Observe weather
Communicate with proximate traffic
Monitor vessel/Cargo condition
Communicate with engine room
Become aware of vessel's capability
Forecast Ice conditions
Assess location and surrounding geography
Obtain weather forcast
Observe other traffic
Download daily ice charts
Ice navigator makes assessments
Obtain map of shipping lanes
Consider predicted/ updated route
Observe radar image
Detect radar image
Assign certified ice navigator
Make shipping schedule



Date: Mar 24,1989 Time: 0001
Abrupt Stop: Grounding
Can not move
Event: The vessel grounded on Bligh Reef
O1: Track line had not changed from radar
O2: Vessel swinging hard starboard
Assess vessel track line
Perform crew work
Inform crew of course
Set new/ maintain course
Assess location and surrounding geography
Make situational assessment
Compute Ice Numeral
Monitor vessel/Cargo condition
Communicate with proximate traffic
Observe weather
Communicate with engine room
Become aware of vessel's capability
Assign ship classification
Observe Ice conditions
Assess location and surrounding geography
Forecast Ice conditions
Obtain weather forcast
Observe other traffic
Download daily Ice charts
Ice navigator makes assessments
Consider predicted/ updated route
Observe radar image
Obtain map of shipping lanes
Make shipping schedule
Assign certified Ice navigator
Detect radar image